SII

Seiko Instruments Inc.

取扱説明書

Xtrax

[krɔ́stræ̀ks]

クロストラックス

マルチサービス・ プラットホーム

NS-4200



ご使用の前に、この取扱説明書をよくお読みの上、正しくお取り扱いください。
お読みになった後も必要なときすぐに見られるよう、大切に保管してください。

セイコーインスツルメンツ株式会社

U00060232400　　2001年　12月
U00060232401　　2002年　 7月

本装置を廃棄する時は、地方自治体の条例に従って処理するようお願い致します。詳しくは、各地方自治体にお問い合わせください。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

高調波ガイドライン適合品
本装置は、通商産業省通知の家電・汎用品高調波抑制対策ガイドラインに適合しています。

はじめに

このたびはNS-4200マルチサービス・プラットホーム（以後、本装置と呼びます）をお買い上げ頂き、まことにありがとうございます。
本書では、システムソフトウェアのインストールおよびセットアップの方法などを説明しています。
本書は、ネットワークに関する知識を持ったネットワーク管理者を対象に、以下のような構成で説明しています。

1章　機能や各部の名称など本装置の概要を説明しています。
2章　本装置の立ち上げ/シャットダウンの方法を説明しています。
3章　本装置のセットアップ手順と本装置のセットアップファイルの概要について説明しています。
4章　本装置の各機能、動作を設定するためのセットアップファイルの設定方法について、システム構成例に基づいて説明しています。
5章　本装置で使用するセットアップファイルの文法についてまとめて説明しています。
6章　本装置の状態表示、セットアップファイルの確認などを行う各種コマンドの使用方法を説明しています。
7章　トラブルが発生したときの対処方法を説明しています。
付録　付録Aではファイルの編集を行うエディタの使い方を説明しています。付録Bでは本装置のコンソールあるいはsyslogホストに出力されるメッセージについて説明しています。付録Cでは本装置がサポートしているRADIUS認証サーバにおけるattributeの設定方法、および本装置がRADIUSアカウントサーバに送信するattributeについて説明しています。付録DではTELNETサーバの設定方法について説明しています。また付録Eでは、バージョンアップの手順について説明しています。

まず、次の「安全上のご注意」および「取り扱い上の注意」をお読みになってから、本書を読み進めてください。

注意　本書は、NS-4200-10向けに書かれています。
NS-4200-30をご使用の場合は、以下の点にご注意ください。
・モデム通信機能は、サポートされません。
・ISDN同期64Kでの通信機能は、サポートされません。
・高速ディジタル回線は、ご利用になれません。

安全上のご注意

ご使用の前に、この「安全上のご注意」をよくお読みの上、本装置を安全に正しくお使いください。

本書では、本装置を安全に正しくお使いいただくため、または機器の損傷を防ぐため、次の記号を使って注意事項を喚起しています。

これらの記号表示の意味は次のとおりです。内容をよく理解して、本書をお読みください。

⚠ 警告	**この表示の内容を無視して、誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。**
⚠ 注意	**この表示の内容を無視して、誤った取り扱いをすると、人が傷害を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。**

絵表示の例



△記号は、注意（危険・警告を含む）を促す内容があることを告げるものです。
左の表示例は「**警告または注意事項**」があることを表しています。



⃠記号は、禁止の行為であることを告げるものです。
左の表示例は「**分解禁止**」を表しています。



●記号は、行為を強制したり、指示する内容を告げるものです。
左の表示例は**「電源プラグをコンセントから抜く」**ことを表しています。

⚠ 警告

本装置を分解したり、改造したりしないでください。
発熱・発火・感電や故障の原因になります。

湿気の異常に多い場所や水などの液体のかかる場所では、絶対に使用しないでください。
火災や感電、故障の原因になります。

本装置の内部やすき間に、金属片を落としたり、水などの液体をこぼさないでください。
火災や感電、故障の原因になります。

濡れた手で、電源ケーブルなどを接続したり、はずしたりしないでください。
感電の原因になります。

本装置の吸気口や排気口をふさがないでください。
発熱などにより、火災や感電、故障の原因になります。

次のような場合は、電源を切り、電源プラグをコンセントから抜いてください。
異常状態のまま使用すると、事故や火災の原因になります。

- ◆ オプションを取り付けるとき
- ◆ お手入れするときや異常時の処置を行うとき
- ◆ 異臭がする、煙が出た、または異常音が発生したとき
- ◆ 本装置の内部やすき間に、金属片や水などの液体が入ったとき
- ◆ 本装置を落としたり、装置の外面が破損したとき
- ◆ 本装置のコンソールに以下のWarningメッセージが表示されたとき（このメッセージは、本装置が冷却ファンの停止を検出したことを示します）

```
@W(1/25 14.15.02):FAN:detect FAN alarm
!!!!! CAUTION : NEED TO POWER DOWN IMMEDIATELY !!!!!
```

⚠ 注意

次のようなことは、絶対に行わないでください。
守らないと、火災や感電、事故または故障の原因になります。

◆ 本装置の上に物を置かないでください。
◆ 本装置をたたいたりなどして、衝撃を与えないでください。
◆ 不安定な場所には置かないでください。
◆ ケーブルの上に物を載せたり、ケーブルをねじったり、強く引っ張ったりしないでください。

次のような場所には設置しないでください。
故障の原因になります。

◆ 直射日光の当たる場所
◆ 温度、湿度の変化の激しい場所
◆ ほこりの多い場所
◆ 振動のある場所
◆ 冷暖房機器の近く
◆ 通風口からの風があたる場所

次のことは、必ずお守りください。
守らないと、火災や感電、事故または故障の原因になります。

◆ 必ず指定の電源電圧（AC100V）で使用してください。
◆ ケーブルを接続するときは、本装置および接続機器の電源を切ってから行ってください。

電源ケーブルは、必ず接地してください。
接地しないと火災や感電の原因になります。

このほか、各項で示す警告／注意事項についてもお守りください。

取り扱い上の注意

- RESETスイッチを押すときはボールペンの先など、先の細いもので押してください。ただし、シャープペンシルは使用しないでください。シャープペンシルの芯が折れて中に入ると、故障の原因となります。

- 本装置の外装が汚れたときは、水で薄めた中性洗剤に柔らかい布を浸し、よくしぼってから拭き取り、さらに乾いた布で拭いてください。

- 本装置を電源OFFした後、再度電源をONする場合には、10秒以上経過してから電源をONにしてください。あまりはやく電源をONにすると、正常に本装置がリセットされない場合があります。

- メモリカードを抜くときには、イジェクトボタンを押して抜いてください。

- 次のようなことは、絶対に行わないでください。
  本装置やメモリカードの故障またはメモリカードの内容が破壊される原因になります。

  ・メモリカードアクセスランプが点灯しているときに、メモリカードを抜き差ししたり、電源を切ったり、RESETスイッチを押したりしないでください。
  ・メモリカードのコネクタ部に、手や金属で直接触れないでください。
  ・メモリカードを落としたり、曲げたり、分解しないでください。
  ・メモリカードは変形、反りなどによって品質低下を招く恐れがありますので、直射日光の当たるところ、暖房器具の近くなどの高温になる場所、また湿気やホコリの多い場所には置かないでください。

目　次

4章　各種機能の設定方法　4-1

6章　コマンド・リファレンス　6-1

7章　トラブルシューティング　7-1

図

表

1章

装置概要

1章では、システムソフトウェアのインストールやセットアップを行ううえで必要な情報を説明しています。作業を始める前に必ずお読みください。

本章の内容

1.1 機能、特長

(1) リモートルータ

NS-4200-10は、複数の拠点やユーザがISDN回線を経由して端末型接続でセンターサイトのネットワークにアクセスするためのアクセスサーバの機能を提供します。また遠隔地にあるイーサネットLAN間を、ISDN回線や高速ディジタル回線を介して接続するネットワーク型接続のリモートルータとしても使用できます。
NS-4200-30は、PIAFS通信機能に特化したモデルです。ISDN回線上のPIAFS通信を使用して、アクセスサーバ機能およびリモートルータ機能を提供します。
ルーティング可能なプロトコルは、IPプロトコルです。

(2) マルチスロット構成

本装置は、マルチスロット構成になっており、システム構成に応じた柔軟な通信機能のサポートが可能です。

(3) PIAFS通信機能

本装置は、NS-421-10/30 DSP拡張ボードを使用することによって、PRIポート上で、PHS端末との間でPIAFS (PHS Internet Access Forum Standard)プロトコルを使用したデータ通信を行うことが可能です。

(4) モデム通信機能

本装置は、ディジタルモデム機能をサポートしたNS-421-10 DSP拡張ボードを使用することによって、PRIポート上でモデム端末とのデータ通信を行うことが可能です。

(5) 自動接続／切断機能

本装置は、ISDN回線を介して接続する接続相手に対するフレームを検出すると、自動的にISDN回線を接続することが可能です。またアイドル監視機能(一定時間以上データが流れていないことを検出する機能)による切断、あるいはセッション監視機能(あらかじめ設定された時間経過したことを検出する機能)による切断を行うことが可能です。

(6) PPP／MP機能

本装置は、各種LANプロトコルをポイントツーポイント回線上で接続するためのリンクプロトコルであるPPP(Point-to-Point Protocol)をサポートしています。
またMP(Multilink Protocol) / BACP (Band width Allocation Control Protocol) もサポートしていますので、複数のリンク(Bチャネル)を使用して、より高速な通信を行うことができます。MP/BACPを使用した場合、BOD(Bandwidth-On-Demand)機能により、トラフィックの増減に応じて自動的にリンクの追加／削除を行うことができます。
BACPでは、MPと違ってリンクの増減に先立って接続相手の了解を得る手続きを定めています。これにより、リンクの追加要求を受け入れた側で、着信のための必要な資源の確保や、着信側の電話番号を相手に通知したりすることができるようになります。

(7) IPアドレス割り当て機能

本装置は、通信相手とのPPP手順において、IPアドレスを通信相手に割り当てることが可能です。この際、通信相手に割り当てるIPアドレスを本装置にプールしておき、プールされているIPアドレスの中から自動的に空いているIPアドレスを割り当てることもできます。

(8) 認証機能

本装置は、ISDN回線からの着信時に、通信相手の電話番号をチェックするCLID認証、およびPPPの認証プロトコルのPAP(Password Authentication Protocol)およびCHAP(Challenge Handshake Authentication Protocol)を使用するPPP認証をサポートしていますので、セキュリティを確保することができます。

(9) RADIUSサーバ対応

本装置は、あらかじめ本装置に登録されているRADIUS認証サーバを使用してCLID認証、およびPPP認証を行うことができます。また、RADIUSアカウントサーバに対してアカウントを記録することができます。

(10) IPパケットフィルタ機能

本装置がフォワーディングするIPパケットを、IPパケットの宛先アドレス、送信元アドレス、上位層のポート番号などによりフィルタすることができます。

(11) コールバック機能

本装置は、CBCP (CallBack Control Protocol : Microsoftコールバック方式)と、独自方式による無課金コールバックをサポートしています。本機能を利用することによって、セキュリティの強化あるいは通信コストの一括管理を行うことが可能になります。

(12) ダイナミックルーティング機能

本装置は、ダイナミックルーティングの機能としてRIP(Routing Information Protocol)バージョン1、バージョン2をサポートしています。

(13) ネットワーク管理プロトコル

ネットワーク管理用のプロトコルとして、SNMP（Simple Network Management Protocol）をサポートしています。

(14) syslog機能

本装置はあらかじめ設定されているsyslogホストに対して、エラーメッセージ、およびトレースメッセージを出力することができます。

(15) 自動復帰機能

万一、本装置内部に障害が発生した場合でも、ウォッチドッグタイマによりこれらの障害を監視し、自動的にリブートする機能があります。

1.2　各部の名称と機能

ここでは、本装置の本体、および各種拡張ボードの各部の名称と機能について説明します。

1.2.1　本体

本体には、LAN(イーサネット)ポート、コンソールポート、設定情報を保存するメモリカードスロット、各種ステータスを表示するランプ、および拡張ボードを格納する拡張ボードスロットなどがあります。
本装置は、4つの拡張ボードスロットを装備しており、システム構成に応じてNS-420 PRI拡張ボードを1枚とNS-421-10/30 DSP拡張ボードを1〜2枚まで装着することができます。ただしISDN回線や高速ディジタル回線に接続するためには、NS-420 PRI拡張ボードが必要になります。

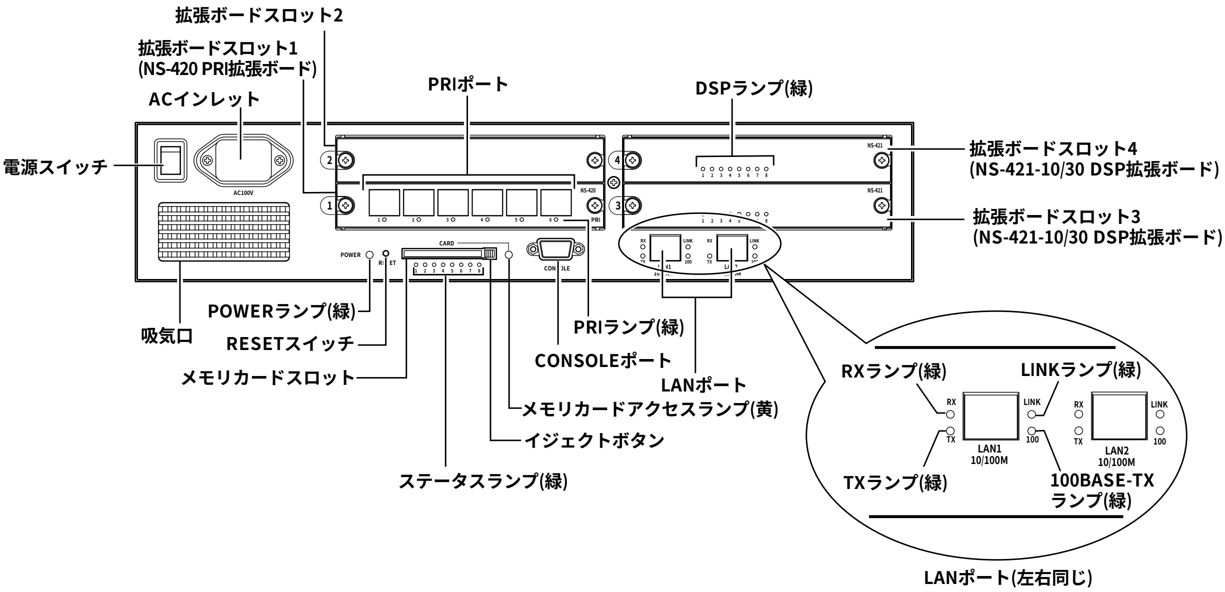


図1-1　本体の各部の名称

① ランプ (POWER／ステータス)

名　称	色	機　　能
POWERランプ	緑	電源がONのときに点灯します。
ステータスランプ	緑	ブートの状況を表示します。 詳しくは「**2.2　立ち上げ**」を参照してください。

② メモリカードスロット／イジェクトボタン／アクセスランプ

コンパクトフラッシュアソシエーションの規格に準拠したメモリカードの挿入用スロットです。セットアップの内容を記録するときに使用します。イジェクトボタンとアクセスランプが付いています。

③ RESETスイッチ

本装置をリブートするときに押します。

④ インタフェースポート

名　称	機　　能
CONSOLEポート	端末との接続用ポート (RS-232C準拠) です。 端末からセットアップを行ったり、本装置のコンソールメッセージが出力されます。
LAN1ポート *	イーサネットHUBとの接続用ポートです。
LAN2ポート *	イーサネットHUBとの接続用ポートです。

＊ LAN1／LAN2ポートは、10BASE-Tおよび100BASE-TXをサポートしており、10BASE-Tまたは100BASE-TXの自動認識が可能です。またLAN1／LAN2ポートは独立したイーサネットポートですので、独立したイーサネットセグメントに接続できます。

⑤ ランプ (LINK / 100BASE-TX / RX / TX)

名　称	色	機　　能
RXランプ	緑	LAN1／LAN2ポートでデータを受信したときに点灯します。
TXランプ	緑	LAN1／LAN2ポートでデータを送信したときに点灯します。
LINKランプ	緑	LAN1／LAN2ポートがリンクテストパルスを検出しているときに点灯します。
100BASE-TXランプ	緑	LAN1／LAN2ポートが100BASE-TXで接続されたときに点灯します。10BASE-Tの場合には消灯します。 **（注）ケーブルを接続していないときにも点灯します。**

⑥ 電源スイッチ

本装置の電源をON / OFFします。
｜と表示されている側を押し込むとON、○と表示されている側を押し込むとOFFになります。

⑦ ACインレット

電源ケーブルを接続します。

1.2.2　NS-420 PRI拡張ボード

NS-420 PRI拡張ボードは、I.431の一次群インタフェースISDN回線や高速ディジタル回線に接続するPRIポートを装備しています。

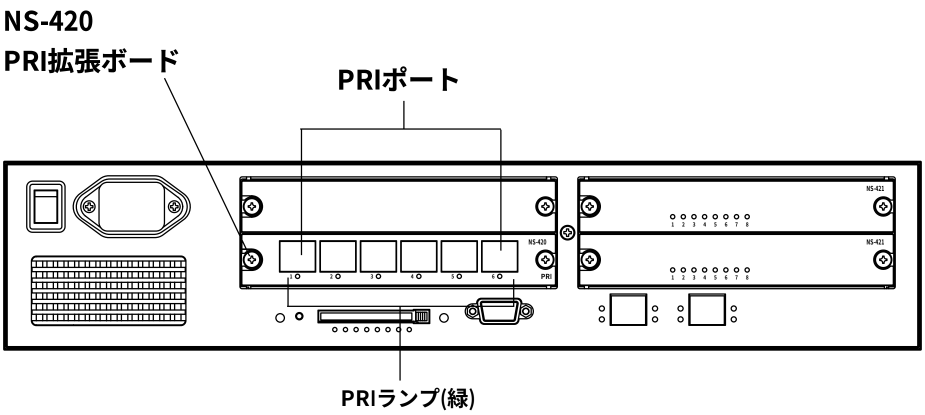


図1-2　NS-420 PRI拡張ボードの各部の名称

名　称	色	機　　能
PRIポート	—	I.431のISDN回線や高速ディジタル回線との接続用ポートです。
PRIランプ	緑	PRIポートのレイヤ１の同期が確立している場合に点灯します。

1.2.3 NS-421-10/30 DSP拡張ボード

NS-421-10 DSP拡張ボードは、モデム機器とのデータ通信を可能にするディジタルモデム機能およびPHS端末との間でPIAFSプロトコルを使用してデータ通信を可能にするPIAFS機能を実現するボードです。
NS-421-30 DSP拡張ボードは、PIAFS機能のみを実現するボードです。

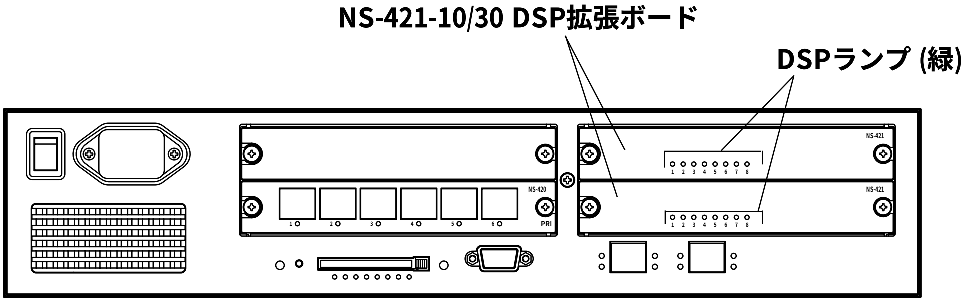


図1-3 NS-421-10/30 DSP拡張ボードの各部の名称

名　称	色	機　　能
DSPランプ	緑	DSP拡張ボードの状態を表示します。

2章

立ち上げ

2章では、本装置を設置した後、システムソフトウェアを立ち上げセットアップを行える状態にするまでの手順、および本装置の動作を終了させる手順について説明しています。
本装置を初めて使用するときには、必ずお読みください。

本章の内容

2.1　端末との接続（CONSOLEポート）

CONSOLEポートは、本装置のセットアップを行ったり、本装置のログ情報などのコンソールメッセージが出力されるポートです。
本装置を初めて使用するときには、本装置のCONSOLEポートに接続した端末から、セットアップを行ってください。

本装置のCONSOLEポートはDTE仕様です。添付のコンソールケーブルを使ってPC/AT仕様のパソコンのCOMポートと接続してください。さらにパソコン上でターミナルソフトを起動して本装置のセットアップを行ってください。

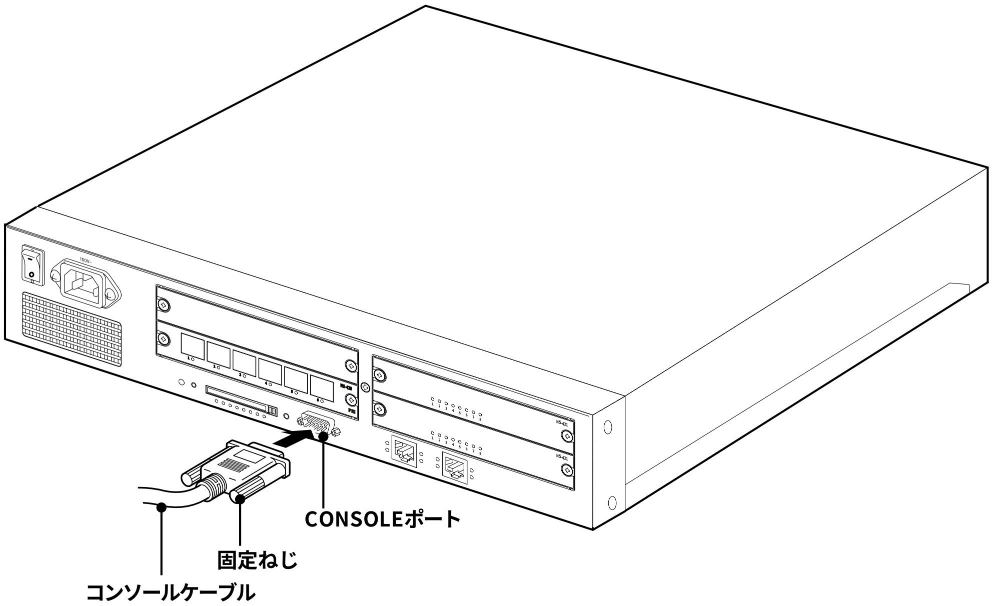


図2-1　端末との接続

表2-1にCONSOLEポートの仕様を示します。接続する端末の設定をこの仕様に合わせてください。

表2-1　CONSOLEポート仕様

項　目	仕　　様
インタフェース	RS-232C（DTE仕様）インタフェース
伝送速度	9600bps
データ長	8ビット
パリティ	なし
ストップビット	1ビット
フロー制御	XON / XOFF
コネクタ	D-SUB 9ピン　オス

2.2　立ち上げ

① 本体に付属のセットアップカードを**図2-2**のように、メモリカードラベルを上にしてメモリカードスロットに差し込みます。溝にそって水平に差し込んでください。

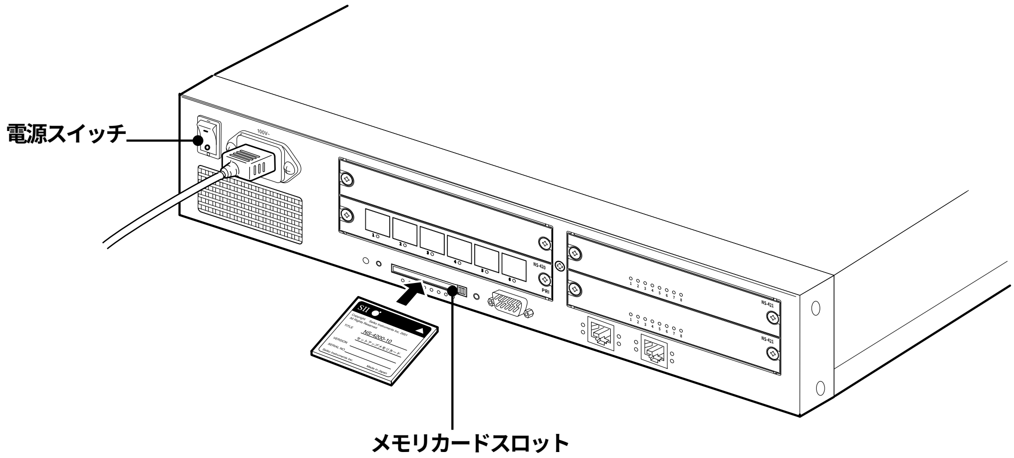


図2-2　セットアップカードの挿入

注　意　　**メモリカードが溝から外れたまま無理に差し込まないでください。溝から外れたまま差し込むと、コネクタのピンが損傷し故障の原因になります。**

注　意　　**セットアップカードは、「SII ●•」が印刷されたラベル面を上にしてメモリカードスロットに差し込んでください。**

注　意　　**セットアップカードは奥まで確実に押し込んでください。**

② 電源スイッチをオンにします。

注意

- **次のことを必ず守ってください。守らないと、火災や感電、事故および故障の原因になります。**
  - **・電源には必ずAC100Vの電源を使用してください。**
  - **・電源ケーブルは必ず付属の電源ケーブルを使用してください。**
  - **・電源ケーブルは必ず接地してください。**
  - **・濡れた手で、電源ケーブルを接続したり、外したりしないでください。**

③ 正常に立ち上がったかどうかを確認します。
電源スイッチをオンにすると、**表2-2**の手順でブートが行われます。ブートが正常に終了すると、ステータスランプ1〜4が全て消灯します。

表2-2　ステータスランプ

ステータスランプ								本装置の状態
1	2	3	4	5	6	7	8	
●	●	●	●	●	●	●	●	電源スイッチON直後
●	○	○	○	○	○	○	○	自己診断テスト(POC)実行中(約10秒)
○	●	○	○	○	○	○	○	拡張ボードの自己診断テスト実行中
○	○	●	○	○	○	○	○	ブート実行中
○	○	○	●	○	○	○	○	ブート実行中2
○	○	○	○	○	○	○	○	ブート正常終了

●：点灯　○：消灯

ステータスランプ1〜4が点滅または点灯したままのときは本装置の故障と考えられます。
「7章トラブルシューティング」にしたがって対処してください。

④ システムソフトウェアが立ち上がると、CONSOLEポートに接続した端末に「login:」が表示されます。

正常に立ち上がったら、**3章**にしたがってセットアップをしてください。

2.3　シャットダウン

本装置の電源をオフにする場合には、shutdownコマンドを実行してシステムソフトウェアを終了してください。

注　意　　**writeコマンドが終了していない状態で、電源をオフにするとセットアップカードの内容が破壊される場合があります。**

① 本装置にログインして、スーパーユーザになります。（**3.1**参照）
② shutdownコマンドを実行します。
③ システムソフトウェアが終了すると、本体正面のステータス4ランプが点滅します。この状態になってから電源をオフにしてください。

```
login: userx↓                                                  下線部を入力
passwd:___________↓
(1)ns> su↓
passwd: ________↓
#shutdown↓
Do you realy want to shutdown  [Y/N]?y↓
```

↓は「CR」キャリッジリターンを表す

3章

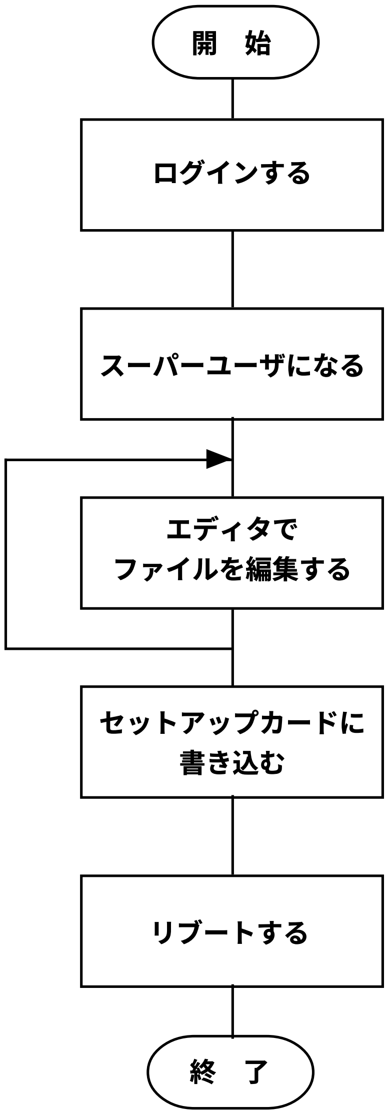
セットアップの手順とセットアップファイル

3章では、本装置のセットアップ手順、セットアップファイルの概要、および本装置を使用する上で必ず設定する必要のあるセットアップファイルについて説明します。各セットアップファイルの詳細な設定方法については、本章をお読みのうえで、**4章**、**5章**を参照してください。

本章の内容

3.1　セットアップ手順

本装置のセットアップ手順を**図3-1**に示します。



CONSOLEポートまたはリモートからtelnetでログインします。本装置に登録されたユーザ名とパスワードを指定します(**3.1.1**参照)。ユーザ名の追加、削除はauthコマンド(**9章**参照)で行えます。

セットアップファイルを編集するには、スーパーユーザになる必要があります(**3.1.2**参照)。

ここでの編集は一時的にメモリ上のファイルを変更するものです。電源を切ると変更内容は失われます(**3.1.3**参照)。

編集したファイルをセットアップカードに書き込みます。電源を切っても変更内容は失われず、次のブート時に変更が反映されます(**3.1.4**参照)。セットアップファイルの内容を工場出荷時に戻す場合はclearコマンド(**6章**参照)を使用します。

更新されたセットアップはリブートによって有効になります(**3.1.5**参照)。一部の設定変更の場合にはreloadコマンド(**6章**参照)で有効になるものがあります。

図3-1　セットアップ手順

参　考　日付および時刻を変更する場合はdateコマンド(**6章**参照)を使用します。ftpを利用してセットアップファイルをセーブ／リストアする場合はloadコマンド(**6章**参照)を使用します。
showコマンド(**6章**参照)で、セットアップファイルの内容を見ることができます。

3.1.1　ログイン／ログアウト

ここでは、CONSOLEポートに接続した端末またはネットワーク上のホストから、本装置にログイン / ログアウトする方法を説明します。

(1) ログインの方法

ユーザ名、パスワードを入力して本装置にログインします。

ログイン手順 (ユーザが設定されている場合)

```
login: xxxx↓                          ユーザ名を入力
passwd: ______↓                       設定されているパスワードを入力
(1)ns>
```

↓は「CR」キャリッジリターンを表す

工場出荷時には、ユーザ「somebody」のみが設定されています。ユーザ「somebody」にはパスワードが設定されていませんので以下のようにログインします。

```
login: somebody↓
passwd:↓
(1)ns>
```

somebodyにパスワードを設定する場合には、以下のようにpasswdコマンドで設定します。確認のため2回同じパスワードを入力します。

```
(1)ns> passwd↓
Enter New Password ? _______↓
Re-Enter New Password ? ______________↓
(1)ns>
```

■プロンプトについて

本装置にログインした際に表示されるプロンプトには、以下の5種類があります。

工場出荷時の状態でコンソールからログインした場合

```
(1)install>
```

本装置のホスト名をhostnameファイルに設定した後にコンソールからログインした場合

```
(1)ns4200>
```

hostnameファイルで設定したホスト名がプロンプトになる

コンソールからスーパーユーザでログインした場合

```
#
```

telnetで本装置にログインした場合

```
(Px)ns4200>
```

telnetで接続する度に1から順に空いている番号が割り付けられる

shutdownコマンド入力後にコンソールから「CR」キャリッジリターンを入力した場合

```
MON>
```

(2) ログアウトの方法

「lo」コマンドで、本装置からログアウトします。
CONSOLEポートに接続した端末からログアウトした場合には、「login:」が表示され、ログイン待ちの状態になります。
ネットワークからtelnetでログインしている場合には、telnetコネクションが解放され、ホストのプロンプトに戻ります。

CONSOLEポートの端末からログアウトした場合

```
(1)ns> lo↓
login:
```

ネットワークのホストからログアウトした場合

```
(1)ns> lo↓
connection closed by foreign host
host1#
```

ホストのプロンプト　　**このメッセージはホストによって異なる**

3.1.2　スーパーユーザ

本装置のセットアップファイルの編集は、スーパーユーザでなければできません。
CONSOLEポートまたはtelnetでログインした状態では、通常ユーザです。

(1) スーパーユーザにログインする

以下の例のように通常ユーザからsuコマンドを実行すると、「passwd:」が表示されますので、スーパーユーザのパスワードを入力します。ユーザ名とパスワードが正しければ、スーパーユーザのプロンプト(#)が表示されます。

```
(1)ns> su↓
passwd: _______↓
#
```

注 意　　入力したパスワードは表示されません。

工場出荷時には、スーパーユーザにはパスワードが設定されていません。「passwd:」に対してキャリッジリターン「↓」のみを入力してください。

スーパーユーザにパスワードを設定する場合には、以下のようにpasswdコマンドで設定します。
確認のため2回同じパスワードを入力します。

```
#passwd↓
Enter New Password ? _______↓
Re-Enter New Password ? ______________↓
#
```

(2) スーパーユーザからログアウトする

以下の例のようにスーパーユーザからloコマンドを実行すると、通常ユーザに戻ります。

```
#lo↓
(1)ns>
```

3.1.3　エディタによるファイルの編集

エディタを使用してセットアップファイルを編集します。エディタで編集するファイルはメモリ上のファイルなので一時的な編集になります。編集したファイルをセットアップカードに保存するには、**3.1.4**項の操作が必要です。

注　意　　**セットアップカードに保存をしないで本装置の電源をオフにしたり、リブートした場合には、編集した内容は失われます。セットアップカード内のファイルの内容は編集前のままです。**

参　考　　**エディタを使って通信に必要な設定（自局のIPアドレスなど）を行ってリブートすれば、各種セットアップファイルをloadコマンド（ftpクライアント）でワークステーションなどにセーブできます。ワークステーション上で編集後、loadコマンドでリストアし、writeコマンドでセットアップカードに書き込むことができます。**

本装置のエディタは、行単位での編集を行うための簡易的なラインエディタです。このため操作は比較的容易です。
エディタの使い方の詳細については、**「付録A　エディタの使い方」**を参照してください。

(1) エディタの起動

まず、スーパーユーザのプロンプトが表示されている状態で、「edit hosts↓」と入力して、エディタを起動します。hostsファイルの編集モードになり、下図のように行番号とhostsファイルの1行目が表示されます。
カレント行 (現在の編集行) は、1行目になります。

プロンプト　　**↓は「CR」キャリッジリターンを表す**

```
# edit hosts↓                              下線部を入力
0001  #  Internet Hosts file
```

行番号　　**1行目の内容**

なお、行番号は、編集のためにエディタが付加して表示しているもので、実際のセットアップファイルの中身には含まれません。

(2) 設定方法 (エディタの編集)

エディタで使用できるサブコマンドなどを使って、セットアップファイルを編集し設定します。
エディタの編集に必要な操作方法を以下に説明します。

■カレント行の移動

カレント行の移動は、サブコマンドの「n」と「p」で行います。
「n」　　：カレント行を次の行にする。
「p」　　：カレント行を1行前の行にする。

サブコマンド「n」を1回入力すると、次の行が表示され、カレント行は2行目になります。
さらに、「n」を入力すると、ファイルの最後を示す[END]が表示されます。カレント行は2行目のままです。

```
0001  # Internet Hosts file                          「n」を入力
0002  # ddd.ddd.ddd.ddd <hostname>                   「n」を入力
[END]
```

ファイルの最後を示す　**2行目の内容が表示される**

サブコマンド「p」を入力すると、1つ前の行が表示され、カレント行は2行目になります。ここで、「p」を入力すると1つ前の行が表示され、カレント行は1行目になります。
さらに、「p」を入力すると、ファイルの先頭を示す[TOP]が表示されます。カレント行は、1行目のままです。

```
0001  # Internet Hosts file
0002  # ddd.ddd.ddd.ddd <hostname>
[END]                                                「p」を入力
0002  # ddd.ddd.ddd.ddd.<hostname>                   「p」を入力
0001  # Internet Hosts file                          「p」を入力
[TOP]
```

ファイルの先頭を示す　**1行目の内容が表示される**

■行の追加

行の追加は、次のサブコマンドを入力して行います。

「a」　　　：ファイルの最後に1行追加する
「i」　　　：カレント行の前に1行追加する
「o」　　　：カレント行の後に1行追加する

ここでは、ファイルの最後に、行を追加します。
サブコマンド「a」を入力すると、追加する行番号が表示され、行の入力モードになります。

```
[TOP]
0003<
```

「a」を入力

行の入力モードを示す

追加する行番号

ここで、追加する文字列「1.0.0.1　host1↓」を入力してみます。
入力した文字がエコーバックされます。「CR」を入力すると入力モードが終了し、入力した1行が再表示されます。カレント行は入力した行になります。

```
0003< 1.0.0.1  host1 ↓
0003  1.0.0.1  host1
```

下線部を入力

入力した行が再表示される

入力ミスの修正方法

もし、文字列「1.0.0.1　host1」を入力中に、打ち間違いをしたときには「DEL」または「BS」キーを押して、文字を消去してから打ち直してください。

■指定行の内容表示

編集中のファイルの内容を、表示して確認してみます。
サブコマンド「l」(小文字のエル) を入力すると、プロンプト「line>」が表示され、表示範囲の入力モードになります。

```
0003  1.0.0.1  host1                                  「l」を入力
line>
```

表示範囲入力待ちのプロンプト

「1,3↓」を入力して、編集中のファイルの1行目から3行目までを表示してみます。
カレント行は変わりません。

```
line> 1,3 ↓                                           下線部を入力
0001  # Internet Hosts file
0002  # ddd.ddd.ddd.ddd <hostname>
0003* 1.0.0.1  host1
```

カレント行には「*」が表示される

1行目から3行目の内容が表示される

■行の消去

カレント行を1行消去してみます。
サブコマンド「d」を入力すると、カレント行が消去され、
「1 line deleted.」と表示されます。カレント行は、行番号0002の行になります。

```
line> 1,3 ↓
0001  # Internet Hosts file
0002  # ddd.ddd.ddd.ddd <hostname>
0003* 1.0.0.1  host1                                  「d」を入力
1 line deleted.
```

■サブコマンド一覧の表示

サブコマンド「?」を入力すると、エディタで使用できるサブコマンドの一覧を表示することができます。
エディタのサブコマンドの一覧と、現在編集中のファイル名が表示されます。

```
1 line deleted.                                「?」を入力
+----<edit commands>---------------------------+
| t: top line               b: bottom line     |
| n: next line              l: list            |
| p: previous line          s: search string   |
| d: delete line            o: append line     |
| c: change line            y: store line      |
| a: add line               z: recover line    |
| i: insert line            j: jump line       |
| q: quit                   e: exit            |
+----<column edit commands>--------------------+
| ^f: 1 column right        ^b  1 column left  |
| ^t: top column                               |
| ^u: recover column(1 line)                   |
+----<edit file name>--------------------------+
| hosts                                        |
+----------------------------------------------+
```

編集中のファイル名

(3) エディタの終了

エディタの終了もサブコマンドを入力して行います。編集した内容をファイルにセーブするかどうかで使用するサブコマンドが異なります。

■セーブして終了する場合

編集した内容をファイルにセーブしてエディタを終了する場合は、サブコマンド「e」を入力します。
編集した内容がファイルに書き込まれ、エディタが終了します。画面にスーパーユーザのプロンプトが表示され、次のファイルを設定することができます。

```
#
```

「e」を入力

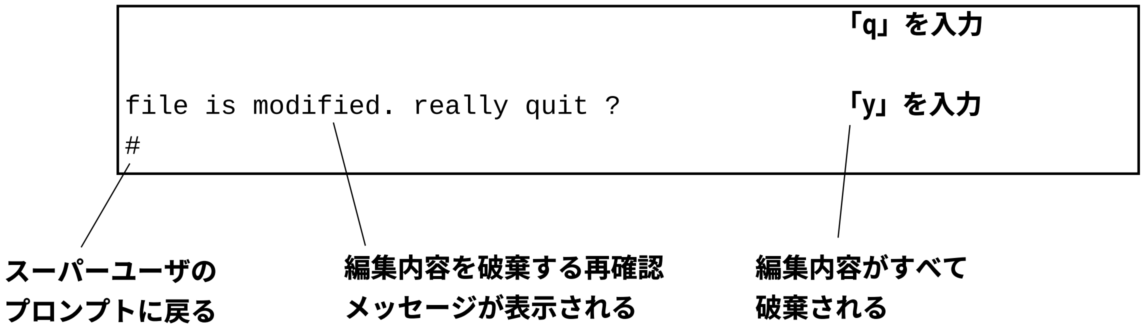
スーパーユーザのプロンプトに戻る

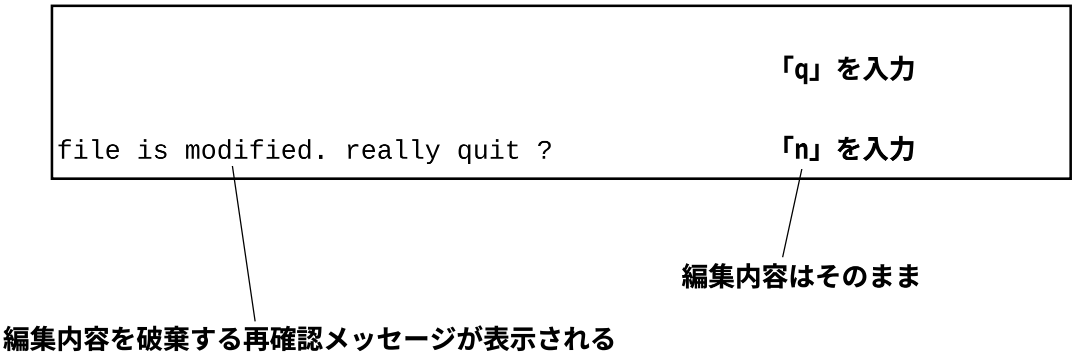
注　意　　**セーブした内容はメモリ上の一時ファイルに書かれます。セットアップカードに保存するにはwriteコマンドを実行してください。writeコマンドを実行しないで、電源をオフにしたり、リブートしたりすると変更内容が失われてしまいます。**

注　意　　**変更した内容は、本装置をリブートすると有効になります。**

■セーブしないで終了する場合

編集した内容をファイルにセーブしないでエディタを終了したい場合には、サブコマンド「q」を入力します。
すでに内容が変更されている場合には、「`file is modified. really quit?`」と表示され、エディタ終了の再確認がされます。ここで文字「y」を入力すると、いま実行したすべての編集内容が破棄されてエディタが終了します。ファイルは編集前のままで、表示はスーパーユーザのプロンプトに戻ります。
また、ここで文字「n」を入力すると、エディタは終了せず編集モードに戻ります。





参　考　　**セットアップファイルの共通規則**

セットアップファイルには、**図3-2**および**表3-1**に示す共通規則があります。特に断わりのない限り、各セットアップファイルはこの規則に従っています。

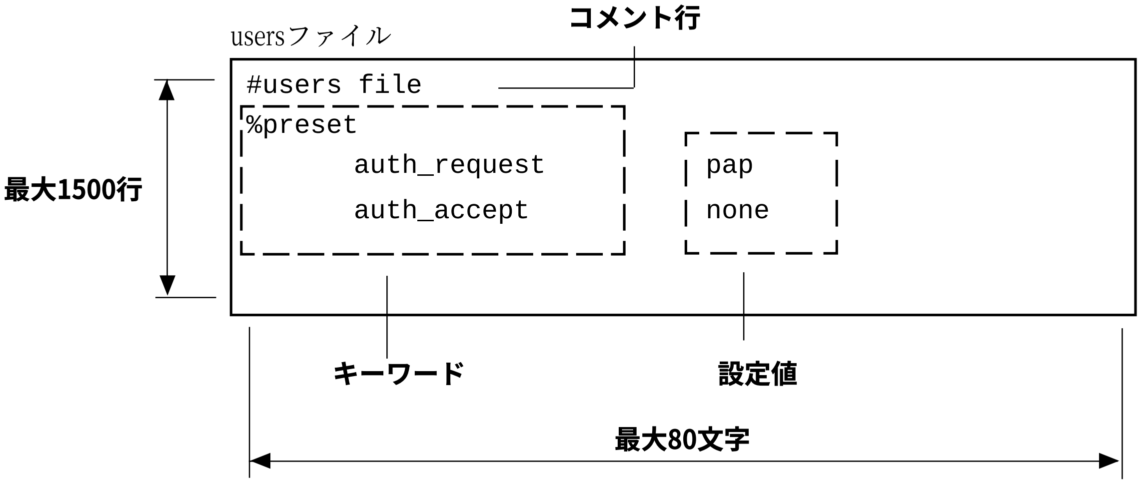


図3-2　セットアップファイル(usersファイル)の例

表3-1　セットアップファイルの共通規則

項　　目	**共通規則**
1行の最大文字数	80文字
1ファイルの最大行数	1500行
使用できる文字	英数字および #%*<>_()などの記号
コメント行	先頭の文字が「#」で始まる行
項の区切り	項目を表すキーワードや設定値の間は、1文字以上のスペースまたはタブで区切る。
キーワード	設定項目を区別するために予め決められている文字列。大文字と小文字は区別される。

項の区切りは1文字以上のスペースまたはタブですから、以下の設定例1と設定例2は同じ設定になります。ただし、設定例2はこの説明のために便宜上用いたもので、通常は設定例1のように読み易い設定にします。

usersファイルの設定例1 (位置揃えした例)

```
%preset
      auth_request   pap
      auth_accept    none
```

usersファイルの設定例2 (位置揃えしてない例)

```
%preset
      auth_request           pap
   auth_accept      none
```

3.1.4　セットアップカードへの保存

エディタで編集した内容をセットアップカードに保存します。保存した内容は、本装置の電源をオフにしても消えません。

```
#write ↓
#
```

注　意　　**writeコマンドの実行中は電源をオフにしたりRESETスイッチを押したりしないでください。セットアップカードの内容が壊れる場合があります。**

3.1.5　リブート

セットアップカードに保存したセットアップの内容を有効にするには、本装置をリブートする必要があります。

スーパーユーザの場合には、rebootコマンドを実行してリブートができます。

```
#reboot ↓
Do you realy want to reboot  [Y/N]?y_↓
```

また、システムソフトをshutdownコマンドで終了してから、電源を入れ直すことでリブートができます。

```
#shutdown ↓
Do you realy want to shutdown  [Y/N]?y_↓
```

注　意　　**シャットダウンの終了を、ステータス4ランプの点滅で必ず確認してください。**

3.2　必ず設定する必要のあるセットアップ項目

本装置では、各機能ごとに分かれたセットアップファイルを編集することによって、動作を指定します。本装置で使用するセットアップファイルと設定内容の一覧を、**表3-2**に示します。

表3-2　セットアップファイル一覧

ファイル名	設定内容
hostname	本装置のホスト名を設定します。
hosts	IPアドレスと対応するホスト名を設定します。
boards	拡張ボードの使用方法を設定します。
interface	ネットワークインタフェースの設定をします。
gateways	スタティックルーティングの設定をします。
ipfilters	IPフィルタを設定します。
netmask	サブネットマスクを設定します。
resolv.conf	DNSのリゾルバを設定します。
snmpconf	SNMPの情報を設定します。
users	ISDN経由で接続する接続相手の設定を行います。
radius	RADIUSサーバとの通信に関する設定を行います。
ippool	IPプール機能を使用する場合に、プールするIPアドレスを設定します。
servers	ブート時に起動させる各種サーバのプログラムを設定します。
rip.conf	RIPの設定を行います。
syslog.conf	syslogの設定を行います。
services	サービス名とポート番号の対応を設定します。

本装置を動作させる場合、まず本装置のホスト名を指定するためにhostnameファイルとhostsファイルを設定します。これらのファイルを設定した後には、本装置の再起動が必要になります。

3.2.1　本装置のホスト名の設定

出荷時の状態では、本装置のホスト名およびIPアドレスが設定されていませんので、CONSOLEポートに接続した端末からeditコマンドを使用して、本装置のホスト名およびそのIPアドレスの設定を行う必要があります。
本装置のホスト名を設定するためには、hostnameファイルにホスト名を設定し、このホスト名に対応するIPアドレスをhostsファイルに設定します。
たとえば、本装置のホスト名が「ns4200」、IPアドレスが「172.31.1.24」の場合、以下のようになります。

hostnameファイル

```
#  hostname
ns4200
```

← 本装置のホスト名を設定します。

hostsファイル

```
#
127.1          localhost   loghost
127.2          noforward
#
172.31.1.24    ns4200
```

← hostnameファイルに設定したホスト名に対応するホスト名とIPアドレスを設定します。

設定が終了したら、セットアップファイルの情報をwriteコマンドでセットアップカードに保存します。rebootコマンドでリブートすることにより、LAN1ポートのイーサネットが使用できるようになります。（この状態では、LAN2ポートは使用できません）

```
# write ↓
# reboot ↓
Do you really want to reboot [y/n] ?  y ↓

（この後システムソフトウェアが立ち上がると、LAN1ポートが使用可能になります）
```

その他のセットアップファイルは、使用環境に応じて本装置のeditコマンドで修正し、reloadコマンドを実行すると、本装置を再起動しなくても設定内容を反映させることができます。

LAN1ポートが使用可能になると、LAN1ポートを利用して、イーサネット上のワークステーションなどからtelnetで本装置にログインし、loadコマンド（ftpクライアント）を使用してセットアップファイルのアップロード／ダウンロードができます。したがってワークステーションにアップロードした本装置のセットアップファイルを、使い慣れたワークステーションなどのエディタで編集して、その後本装置に修正したセットアップファイルをダウンロードし、セットアップカードに保存する（writeコマンド）ことができます。loadコマンドの使用方法は、**「6章　コマンド・リファレンス」**を参照してください。

3.2.2　拡張ボードの使用方法の設定

NS-420 PRI拡張ボードに関して、boardsファイルに設定する必要があります。NS-421-10/30 DSP拡張ボードに関しては、設定する必要はありません。
boardsファイルの詳細な記述方法は**5章**で説明しています。また、システム構成例に基づいたboardsファイルの設定例については**4章**で説明しています。
ここでは、boardsファイルについて簡単に説明します。

boardsファイルは、以下のような構成になっています。

```
%board 1
        %port     1
                  line_type isdn
        %port     2
                  line_type isdn
        %port     3
                  line_type isdn
        %port     4
                  line_type isdn
        %port     5
                  line_type isdn
        %port     6
                  line_type hsd
                  %channel  1
                            slots     1-24
```

拡張ボードスロット番号1の拡張ボードに関する設定

拡張ボード上のポート1に関する設定

ポート（この例ではポート6）内の論理チャネル1に関する設定

最初に、%board分類キーワードで、設定する拡張ボードが挿入されている拡張ボードスロット番号を指定します。次に、%port分類キーワードで、拡張ボード上のポート番号を指定し、そのポートに関する設定を続けて行います。必要に応じて（高速ディジタル回線を使用する場合）、%channel分類キーワードで論理チャネル番号の指定と、その論理チャネルに関する設定を行います。

boardsファイルで使用するキーワードの詳細については、**「5章　セットアップ・リファレンス」**の**「5.3　boardsファイル」**を参照してください。

3.2.3　ISDNで接続する接続相手の設定

本装置を使用して接続相手とISDN回線経由で接続する場合、その接続相手の情報をusersファイルに設定する必要があります。
usersファイルの詳細な記述方法は**5章**で説明しています。またシステム構成例に基づいたusersファイルの設定例については**4章**で説明しています。
ここでは、usersファイルの基本的な概念について簡単に説明します。

usersファイルは、以下のような構成になっています。（このusersファイルの設定は、**4章**の**4.1.1**に記述されているものと同一です。各キーワードの設定内容の意味については**4.1.1**をご覧ください。）

```
%preset
  auth_request       pap
  auth_accept        none
%default
  auth_request       none
  auth_accept        pap
  local_name         tokyo
  local_passwd       aoshima
  connect_on_demand  on
  idle_timeout       90


%user
  remote_name        osaka
  remote_passwd      yokoyama
  remote_tel         06-6666-6666

  interface  isdn0   128.30.0.1     unnumbered
          ppp  address  on    *       *
  destination  128.30.0.0/16  via 128.30.0.1 2


%user
  remote_name        chiba
  remote_passwd      numata
  remote_tel         043-222-2222

  interface  isdn0   130.30.0.1     unnumbered
          ppp  address  on   *       *
  destination  130.30.0.0/16 via 130.30.0.1 2
```

%preset分類キーワード：
着信時の認証が終了するまでの動作を設定します。

%default分類キーワード：
接続相手に共通な設定項目を設定します。

%user分類キーワード：
各接続相手ごとに、接続相手との接続条件を設定します。

(1) 分類キーワード

設定を行う場合には、まず分類キーワードを記述し、その次の行から動作を指定するキーワードを設定します。各分類キーワードは、以下のように使用します。

① %user分類キーワード

- 各接続相手ごとに接続相手との接続情報（認証で使用するユーザ名、パスワード、電話番号、ルーティング情報など）を設定します。
- 接続相手の設定を行う場合、まず分類キーワード「%user」を記述し、次の行からその接続相手との接続情報をキーワードを使用して設定します。複数の接続相手の設定を行う場合、それぞれの相手ごとに分類キーワード「%user」から記述します。
- %user分類キーワードで設定できるキーワードの中で、デフォルト値をもつキーワードをデフォルト値で使用する場合には、そのキーワードを設定する必要はありません。また次に述べる%default分類キーワードで設定されているキーワードの設定値を使用する場合にも、自動的に参照されるため、設定する必要はありません。

② %default分類キーワード

- %default分類キーワードに設定したキーワードは、自動的に全%user分類キーワードに反映されます。したがって%user分類キーワードに記述するキーワードにおいて、複数の接続相手に共通な設定内容は、この%default分類キーワードに記述することによって各%user分類キーワードに設定する手間を省くことができます。

③ %preset分類キーワード

- 本装置がISDNからの着信を検出した場合、何らかの認証手順により接続相手を特定しないと上記%userエントリを参照することはできません。この%preset分類キーワードには、認証により接続相手が特定できるまでの動作条件（認証方法、動作プロトコルなど）を設定します。したがってここに設定された内容は、ISDN回線からの着信から認証手順により接続相手が特定できるまでの間、全接続相手に共通になります。認証手順により接続相手を特定できた後は、%user分類キーワードに記述された情報にしたがって動作します。

usersファイルで使用するキーワードの詳細については、「**5章　セットアップ・リファレンス**」の「**5.10　usersファイル**」を参照してください。

(2) 認証方法

ISDN回線から着信した場合、
・セキュリティの確保
・接続相手の特定
の2つの目的で認証手順が実行されます。

本装置には、以下の3つの認証方法があります。

① CLID認証
・ISDNの着信時に相手の電話番号（発信者電話番号）をチェックします。設定に応じて本装置に登録されていない相手の着信を拒否することができます。
・また電話番号情報から、usersファイルに登録されているその接続相手の%userエントリを特定することができます。この場合ISDN着信処理以後のPPPの接続手順は、%user分類キーワードに記述された内容で動作します。

② PPP認証
・ＩＳＤＮ回線からの着信処理が完了すると、ＰＰＰの接続手順が実行されます。本装置では、PPPの認証フェーズで、PAPあるいはCHAPの認証プロトコルを使用して接続相手の認証を行うことができます。認証プロトコルを実行した結果、接続相手の認証を行うとともに、認証プロトコルで通知される接続相手のユーザ名から、その接続相手の%userエントリを特定することができます。

③ RADIUS認証
・ISDN回線からの着信時に、上記CLID認証およびPPP認証の結果、接続相手の情報を本装置usersファイルから検出できなかった場合、RADIUS認証サーバに問い合わせることができます。RADIUS認証サーバを使用するためには、本装置のradiusファイルにも設定を行う必要があります。
・ＲＡＤＩＵＳ認証サーバに問い合わせた結果接続が許可された場合、その着信を許可し、以後RADIUS認証サーバから通知された接続条件で動作します。

注　意　**本装置では、着信処理においてまず本装置のusersファイルに登録されている接続相手を検索し、接続相手が登録されていなかった場合にRADIUS認証サーバに問い合わせます。したがってRADIUS認証サーバを使用して認証を行う接続相手の情報は、本装置のusersファイルの%user分類キーワードでは設定する必要はありません。**
ただし、着信時の動作は、%preset分類キーワードに設定された内容に従いますので、%preset分類キーワードの設定は行う必要があります。

4章

各種機能の設定方法

4章では、本装置の各機能、動作を設定するためのセットアップファイルの設定方法について、システム構成例に基づいて説明しています。

NS-4200-30をご使用の場合は、高速ディジタル回線をご利用になれませんので、**「4.3　高速ディジタル回線経由でネットワーク型接続を行う場合の基本的な設定」**は、お読みいただく必要はありません。

本章で説明している各セットアップファイルおよびそのキーワードなどの詳細な文法は**5章**でまとめて説明していますので、そちらもご参照ください。

本章の内容

本装置では、各種セットアップファイルを編集することによって、機能および動作を指定します。本装置のセットアップファイルを編集する方法には以下の2種類の方法があります。

(1) 本装置にログインして、本装置のエディタでセットアップファイルを編集する方法

本装置にログインして、本装置上でエディタを使用してセットアップファイルを編集します。
この方法については、**「3.1　セットアップ手順」**および**「付録A　エデイタの使い方」**で説明しています。

(2) 普段使用しているマシンで編集したセットアップファイルを、loadコマンドで本装置にロードする方法

普段使用しているマシンでセットアップファイルを編集した後に、本装置のloadコマンドでセットアップファイルをロードすることができます。この場合、セットアップファイルの置かれているマシンでは、ftpサーバが動作している必要があります。
この方法については、**6章**のloadコマンドを参照してください。

初めて本装置の設定を行う場合、**(1)**の方法で、**「3.2　必ず設定する必要のあるセットアップ項目」**に説明されている、hostnameファイル、hostsファイルを設定してください。これらのセットアップを編集し、writeコマンドでセーブした後に、本装置を一度リブートしてください。

その後本装置が起動した後、使用する機能、動作に応じて必要なセットアップファイルを**(1)**あるいは**(2)**の方法で編集してください。設定が完了した後、reloadコマンドを実行すると、設定内容が本装置に反映され、各種機能が使用可能になります。ただしreloadコマンドを実行した際にエラーメッセージが出力される場合には、再度エラー要因となっているセットアップ項目を確認し、編集してください。

本章では、本装置の各種機能、動作を設定するためのセットアップファイルの設定方法について、各機能ごとにシステム構成例に基づいて説明しています。各項では、システム構成図、本装置のセットアップファイルの設定、および設定内容の解説などが記述されています。
まず、**4.1**項、**4.2**項、**4.3**項で基本的なシステム構成について説明していますので、ご使用になる環境に近い構成例をもとに基本的な設定をしてください。
また、**4.4**項、**4.5**項、**4.6**項では、さらに本装置の応用機能に関する説明をしていますので、必要な場合にはこれらの設定例に基づいてさらに追加機能の設定をしてください。

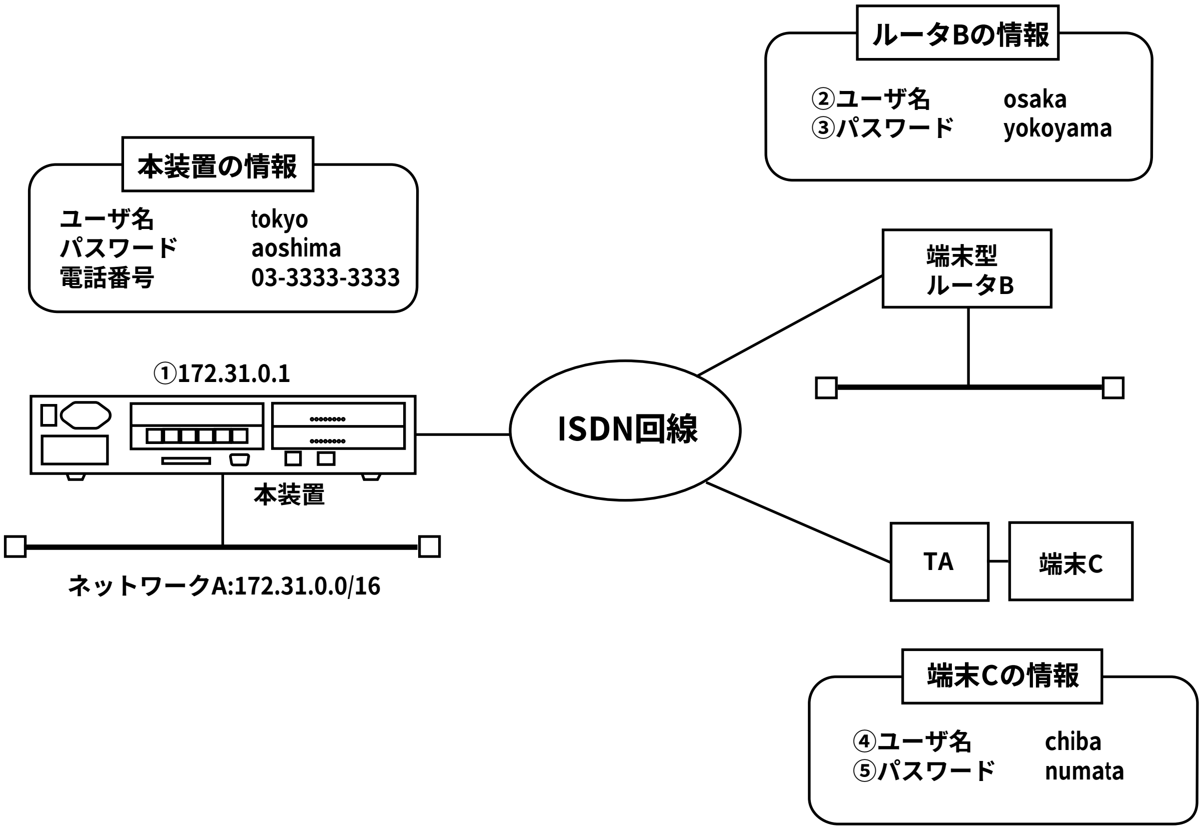
なお、本章で説明している各セットアップファイルおよびそのキーワードなどの詳細な文法については、**5章**にまとめて説明していますので、そちらを参照してください。

さらに本装置の設定を行った後、セットアップファイルの確認、本装置の動作状態、統計情報の表示、および本装置のメンテナンスを行うためのコマンドについては、各コマンドごとに**6章**で説明しています。セットアップファイルの設定が完了し、本装置を動作させる場合には、**6章**も参照してください。

4.1 ISDN経由で端末型接続を行う場合の基本的な設定

4.1.1 接続相手の設定を本装置で行う場合の設定

［構成図］



その他の情報

⑥PPP認証はPAPを使用する。
⑦着信時に本装置のIPアドレスプールからIPアドレスを割り当てる。
⑧IPアドレスプールには、172.31.1.100から23個IPアドレスを登録しておく。
⑨PRI拡張ボードのポート1からポート6までISDN回線で使用する。

[本装置のusersファイルの設定]

```
%preset
      auth_request          pap
      auth_accept           none


%user
      remote_name           osaka
      remote_passwd         yokoyama

      interface  isdn0      *      unnumbered
             ppp  address  on      *  255.255.255.254


%user
      remote_name           chiba
      remote_passwd         numata

      interface  isdn0      *      unnumbered
             ppp  address  on      *  255.255.255.254
```

[構成図の情報との対応]

<着信時の設定>
⑥PPP認証方式

<ルータBに対する設定>
②ユーザ名
③パスワード

⑦論理インタフェースの設定

<端末Cに対する設定>
④ユーザ名
⑤パスワード

⑦論理インタフェースの設定

[本装置のippoolファイルの設定]

```
172.30.1.100/16            23
```

[構成図の情報との対応]

<IPプールの設定>
⑧プールするIPアドレスの設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

①本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
       %port  1
              line_type isdn
       %port  2
              line_type isdn
       %port  3
              line_type isdn
       %port  4
              line_type isdn
       %port  5
              line_type isdn
       %port  6
              line_type isdn
```

[構成図の情報との対応]

⑨拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

［解　説］

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。この設定は全接続相手に共通になります。

・この例では、構成図の⑥の情報から、着信時にはPAPで相手を認証する設定をしています。

<usersファイル：ルータＢに対する設定><端末Ｃに対する設定>

・各接続相手の条件は%user分類キーワードで設定します。

・この例では、まずPAPでPPP認証する場合のユーザ名、パスワードを設定しています。本装置は着信時に%presetキーワードに設定されているPAPによる認証を相手に要求し、相手から送られてくるユーザ名を元にusersファイルを検索し、ルータBあるいは端末Cの%userエントリを特定します。

・%user分類キーワードには、接続相手ごとに論理インタフェースの設定を行います。
この例では、端末型接続で本装置からIPアドレスを割り当てるため、相手IPアドレスが不定ですので、interfaceキーワードにおける相手IPアドレスに「*」を設定します。この設定によって相手と接続した時点で相手に割り当てたIPアドレスを本装置が相手IPアドレスとして設定します。
さらにIPアドレスを本装置のIPアドレスプールから割り当てるための設定として、pppサブキーワードの相手アドレスに「255.255.255.254」を設定します。この設定によって着信時に本装置のIPアドレスプールから空いているIPアドレスを接続相手に割り振ります。
また本装置のIPアドレス（構成図の①）が通知されます。

<ippoolファイル：IPプールの設定>

・本装置にプールしておくIPアドレスは、ippoolファイルに設定します。

・この例では、構成図の⑧の情報から、172.31.1.100から連続する23個のアドレスを設定しています。もし連続しないアドレス、たとえば172.31.1.100から15個、172.31.2.100から８個をプールしたい場合には、以下のように記述します。

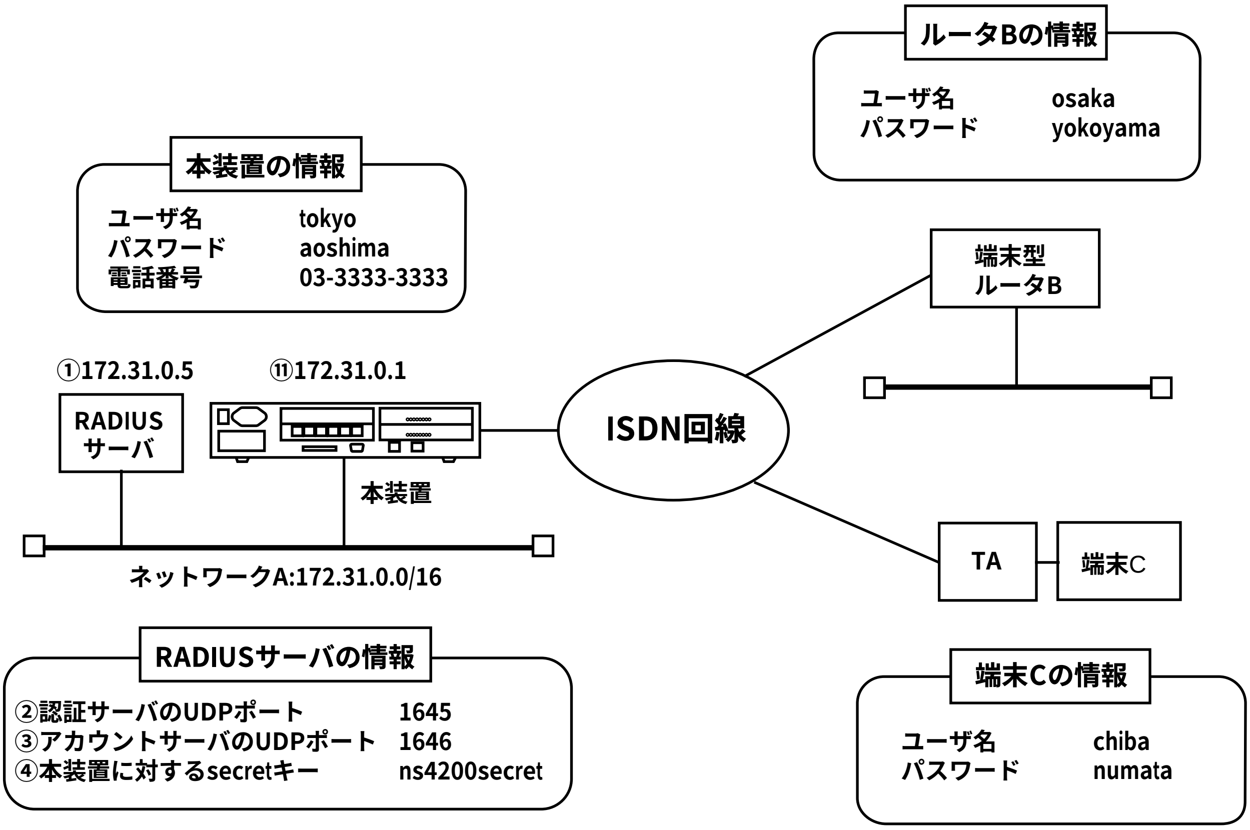
```
172.31.1.100/16      15
173.31.2.100/16      8
```

ただし、設定できるIPアドレスの総数は512個までです。

（ここは空白のページです。）

4.1.2　接続相手の設定をRADIUS認証サーバで行う場合の設定

［構成図］



その他の情報

⑤PPP認証はPAPを使用する。
⑥RADIUS認証サーバを使用して認証を行う。
⑦RADIUSアカウントサーバを使用する。
⑧本装置のIPアドレスプールからIPアドレスを割り当てる。
⑨IPアドレスプールには、172.31.1.100から23個IPアドレスを登録しておく。
⑩PRI拡張ボードのポート1からポート6までISDN回線で使用する。

[本装置のusersファイルの設定]

```
%preset
      auth_request         pap
      auth_accept          none
```

[構成図の情報との対応]

<着信時の設定>
⑤PPP認証方式

[本装置のippoolファイルの設定]

```
      172.31.1.100/16             23
```

[構成図の情報との対応]

<IPプールの設定>
⑨プールするIPアドレスの設定

[本装置のradiusファイルの設定]

```
%radius_auth
      mode          on
      host1         172.31.0.5
      port          1645
      key           ns4200secret

%radius_acct
      mode          on
      host1         172.31.0.5
      port          1646
      key           ns4200secret
```

[構成図の情報との対応]

<RADIUS認証サーバの設定>
⑥認証サーバを使用する
①認証サーバのIPアドレス
②認証サーバのUDPポート
④認証サーバのsecretキー

<RADIUSアカウントサーバの設定>
⑦アカウントサーバを使用する
①アカウントサーバのIPアドレス
③アカウントサーバのUDPポート
④アカウントサーバのsecretキー

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

⑪本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
       %port  1
              line_type isdn
       %port  2
              line_type isdn
       %port  3
              line_type isdn
       %port  4
              line_type isdn
       %port  5
              line_type isdn
       %port  6
              line_type isdn
```

[構成図の情報との対応]

⑩拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

[解　説]

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。RADIUS認証を行う場合もPPP認証の設定が必要です。

・この例では、構成図の⑤の情報から、着信時にはPAPで相手を認証する設定をしています。

<usersファイル：ルータＢに対する設定><端末Ｃに対する設定>

・本装置は、認証の結果からusersファイルの%userエントリを検索し、該当する接続相手が見つからない場合、RADIUS認証サーバに認証要求を行います（ただしradiusファイルにRADIUS認証サーバを使用する設定にする必要があります）。

・この例では、RADIUS認証サーバで認証を行うことから、接続相手（ルータB、端末C）の情報をusersファイルに設定する必要がありません。

<ippoolファイル：IPプールの設定>

・本装置にプールしておくIPアドレスは、ippoolファイルに設定します。RADIUS認証を行う場合でも、IPアドレスプールからIPアドレスを割り当てる場合には、本装置のippoolファイルの設定が必要です。

・この例では、構成図の⑧の情報から、172.31.1.100から連続する23個のアドレスを設定しています。もし連続しないアドレス、たとえば172.31.1.100から15個、172.31.2.100から８個をプールしたい場合には、以下のように記述します。

```
172.31.1.100/16      15
173.31.2.100/16      8
```

ただし、設定できるIPアドレスの総数は512個までです。

<radiusファイル：RADIUS認証サーバの設定>

・RADIUS認証サーバの設定は、radiusファイルに%radius_auth分類キーワードで設定します。

・RADIUS認証サーバを使用するために、modeキーワードでonを設定します。さらにRADIUS認証サーバのIPアドレス、RADIUS認証サーバのUDPのポート番号、RADIUS認証サーバに登録されているsecretキーを設定します。これらの設定はRADIUS認証サーバの設定と合わせてください。

<radiusファイル：RADIUSアカウントサーバの設定>

・RADIUSアカウントサーバの設定は、radiusファイルに%radius_acct分類キーワードで設定します。

・RADIUSアカウントサーバを使用するために、modeキーワードでonを設定します。さらにRADIUSアカウントサーバのIPアドレス、RADIUSアカウントサーバのUDPのポート番号、RADIUSアカウントサーバに登録されているsecretキーを設定します。これらの設定はRADIUSアカウントサーバの設定と合わせてください。

[参　考]

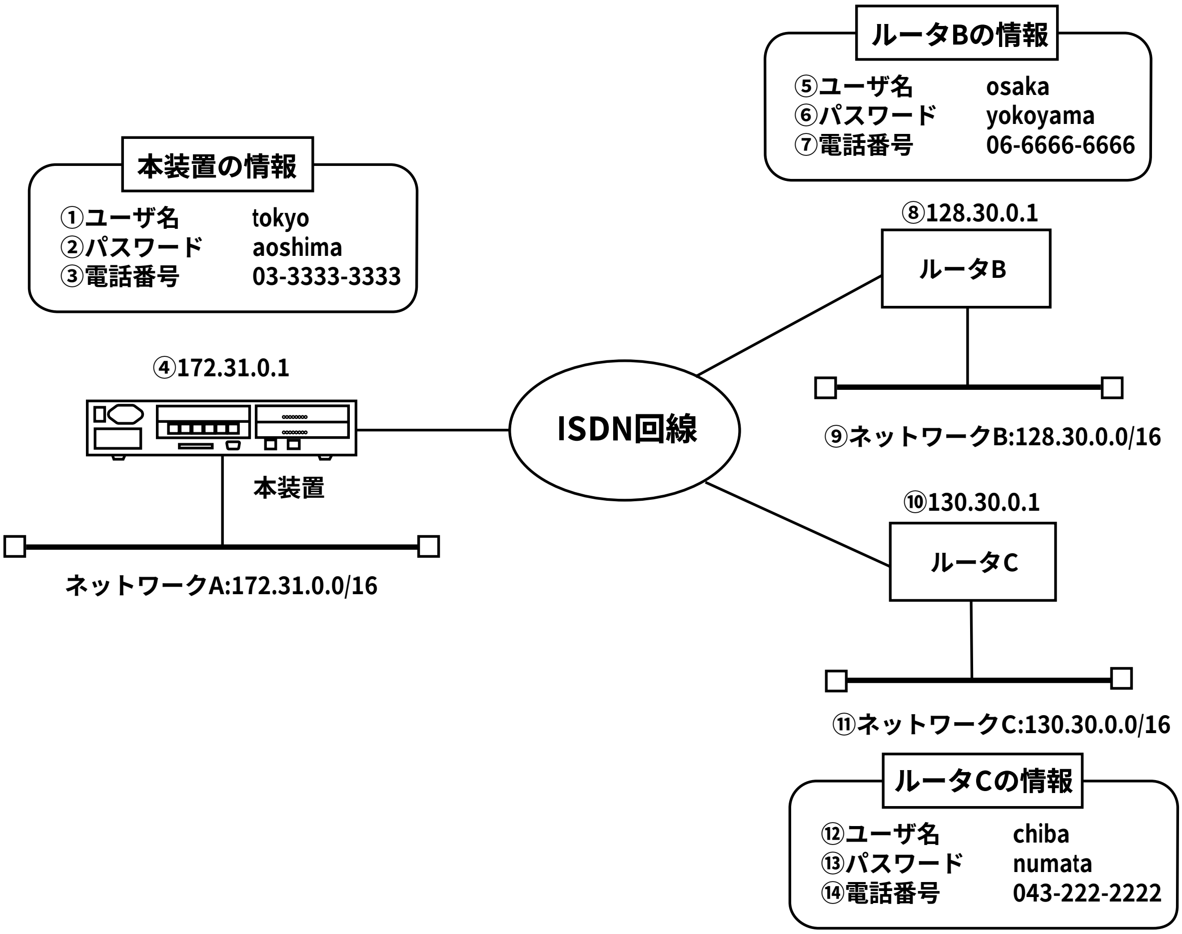
・RADIUS認証サーバの設定については、**「付録C　RADIUSサーバについて」**を参照してください。

（ここは空白のページです。）

4.2　ISDN経由でネットワーク型接続を行う場合の基本的な設定

4.2.1　ISDNインタフェースにIPアドレスを設定しない場合の設定 (PPP認証のみ使用する場合)

［構成図］



その他の情報

⑮プロトコルはPPPを使用する。
⑯PPP認証はPAPを使用し、着信時には相手を認証し、発信時には相手に認証される。
⑰ネットワークB、ネットワークC宛のパケットにより自動発信する。
⑱アイドル監視（90秒）で自動切断する。
⑲PRI拡張ボードのポート1からポート6までISDN回線で使用する。

[本装置のusersファイルの設定]

```
%preset
      auth_request          pap
      auth_accept           none

%default
      auth_request          none
      auth_accept           pap
      local_name            tokyo
      local_passwd          aoshima
      connect_on_demand     on
      idle_timeout          90


%user
      remote_name           osaka
      remote_passwd         yokoyama
      remote_tel            06-6666-6666

      interface  isdn0      128.30.0.1     unnumbered
             ppp  address  on      *       *
      destination  128.30.0.0/16   via  128.30.0.1 2


%user
      remote_name           chiba
      remote_passwd         numata
      remote_tel            043-222-2222

      interface  isdn0      130.30.0.1     unnumbered
             ppp  address  on      *       *
      destination  130.30.0.0/16   via  130.30.0.1 2
```

[構成図の情報との対応]

<着信時の設定>
⑯PPP認証方式（着信）

<ルータB／ルータC共通の設定>
⑯PPP認証方式（発信）

①自局ユーザ名
②自局パスワード
⑰自動発信
⑱アイドル監視時間

<ルータBに対する設定>
⑤ユーザ名
⑥パスワード
⑦電話番号

⑧論理インタフェースの設定

⑨ルーティング情報の設定

<ルータCに対する設定>
⑫ユーザ名
⑬パスワード
⑭電話番号

⑩論理インタフェースの設定

⑪ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

④本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
        %port  1
               line_type isdn
        %port  2
               line_type isdn
        %port  3
               line_type isdn
        %port  4
               line_type isdn
        %port  5
               line_type isdn
        %port  6
               line_type isdn
```

[構成図の情報との対応]

⑲拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

［解　説］

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。この設定は全接続相手に共通になります。

・この例では、構成図の⑯の情報から、着信時にはPAPで相手を認証し、相手からの認証はされない設定をしています。

<usersファイル：ルータB／ルータC共通の設定>

・各接続相手に共通な設定は、%default分類キーワードに設定することによって、各接続相手ごとに設定する必要がなくなります。ここに設定されているキーワードは、<ルータBに対する設定>、<ルータCに対する設定>にそれぞれ記述してもかまいません。

・この例では、共通な設定項目として、

構成図の情報⑯：発信時には本装置からは認証を要求せず、相手からPAP認証要求を受け入れる。

構成図の情報⑰：自動発信する。

構成図の情報⑱：アイドル監視を90秒にする。

構成図の情報①、②：相手からPAP認証される場合の自局ユーザ名、パスワードなどを設定しています。

<usersファイル：ルータBに対する設定>
<usersファイル：ルータCに対する設定>

・各接続相手の条件は%user分類キーワードで設定します。

・この例では、まずPAPでPPP認証する場合のユーザ名、パスワードを設定しています。本装置は着信時に%presetキーワードに設定されているPAPによる認証を相手に要求し、相手から送られてくるユーザ名を元にusersファイルを検索し、ルータBあるいはルータCの%userエントリを特定します。

・%user分類キーワードには、接続相手ごとに論理インタフェースの設定、ルーティング情報の設定を行います。この情報をもとに、接続時に接続相手との間のデータ転送のためのルーティングテーブルを作成し、IPパケットのフォワーディングが可能になります。

・この例は、ISDNインタフェースにIPアドレスを設定しない条件ですので、interfaceキーワードでunnumberedの設定を行っています。したがって自局IPアドレスは設定せず、また相手IPアドレスは相手ルータのIPアドレスを設定します。

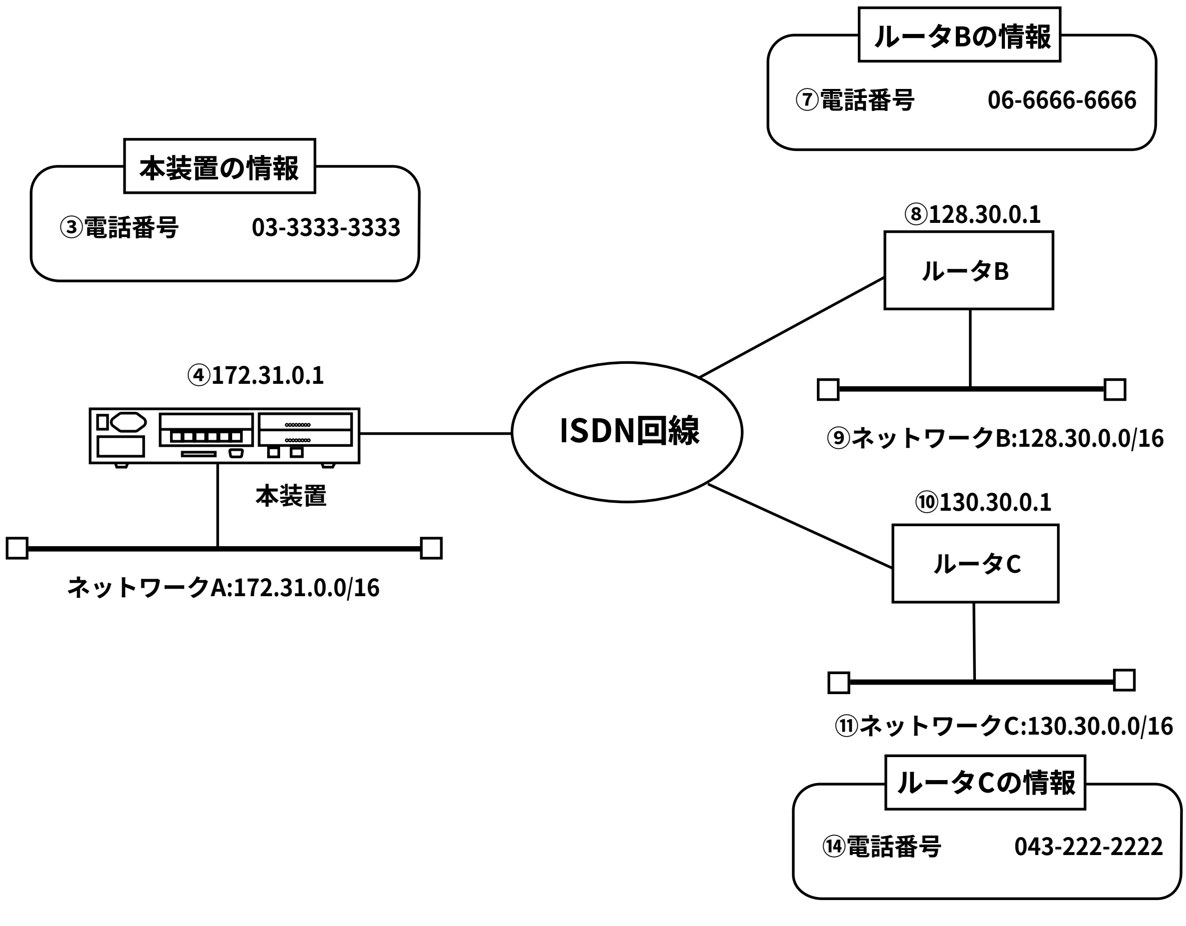
また、pppサブキーワードでPPP接続フェーズのIPCPのアドレスネゴシエーションの設定を行います。この設定は相手ルータの設定と合わせる必要があります。この例のように「ppp address on * *」と設定することによって、本装置は自身のIPアドレス（構成図の④）を送信し、また相手から送信されるIPアドレス（構成図⑧あるいは⑩）を受け入れます。

・さらに相手ネットワークへのルーティング情報を、destinationキーワードで設定します。この時経由するルータのIPアドレスには、interfaceキーワードで指定した相手IPアドレスを指定します。

（ここは空白のページです。）

4.2.2 ISDNインタフェースにIPアドレスを設定しない場合の設定 (CLID認証のみ使用する場合)

［構成図］



その他の情報

⑮プロトコルはPPPを使用する。
⑯CLID認証のみを使用し、PPP認証は使用しない。
⑰ネットワークB、ネットワークC宛のパケットにより自動発信する。
⑱アイドル監視（90秒）で自動切断する。
⑲PRI拡張ボードのポート1からポート6までISDN回線で使用する。

[本装置のusersファイルの設定]

```
%preset
      clid_auth            must

%default
      connect_on_demand    on
      idle_timeout         90


%user
      remote_tel           06-6666-6666

      interface  isdn0     128.30.0.1    unnumbered
             ppp  address  on      *       *
      destination  128.30.0.0/16   via   128.30.0.1 2


%user
      remote_tel           043-222-2222

      interface  isdn0     130.30.0.1    unnumbered
             ppp  address  on      *       *
      destination  130.30.0.0/16   via   130.30.0.1 2
```

[構成図の情報との対応]

<着信時の設定>
⑯CLID認証

<ルータB／ルータC共通の設定>
⑰自動発信
⑱アイドル監視時間

<ルータBに対する設定>
⑦電話番号
⑧論理インタフェースの設定
⑨ルーティング情報の設定

<ルータCに対する設定>
⑭電話番号
⑩論理インタフェースの設定
⑪ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

④本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
       %port  1
              line_type isdn
       %port  2
              line_type isdn
       %port  3
              line_type isdn
       %port  4
              line_type isdn
       %port  5
              line_type isdn
       %port  6
              line_type isdn
```

[構成図の情報との対応]

⑲拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

［解　説］

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。この設定は全接続相手に共通になります。

・この例では、構成図の⑯の情報から、着信時にはCLID（発信者電話番号）で接続相手を認証する設定になっています。したがってISDN回線から着信を検出した時点で、usersファイルに設定されている発信者の電話番号からルータBあるいはルータCの%userエントリが特定されます。

<usersファイル：ルータB／ルータC共通の設定>

・各接続相手に共通な設定は、%default分類キーワードに設定することによって、各接続相手ごとに設定する必要がなくなります。ここに設定されているキーワードは、<ルータBに対する設定>、<ルータCに対する設定>にそれぞれ記述してもかまいません。

・この例では、共通な設定項目として、

　　構成図の情報⑰：自動発信する。

　　構成図の情報⑱：アイドル監視を90秒にする。

などを設定しています。

<usersファイル：ルータBに対する設定>
<usersファイル：ルータCに対する設定>

・各接続相手の条件は%user分類キーワードで設定します。

・この例では、相手電話番号をremote_telキーワードで設定しています。この電話番号は、発信用の電話番号として使用されるとともに、着信時のCLID認証用の電話番号としても使用されます。

・%user分類キーワードには、接続相手ごとに論理インタフェースの設定、ルーティング情報の設定を行います。この情報をもとに、接続時に接続相手との間のデータ転送のためのルーティングテーブルを作成し、IPパケットのフォワーディングが可能になります。

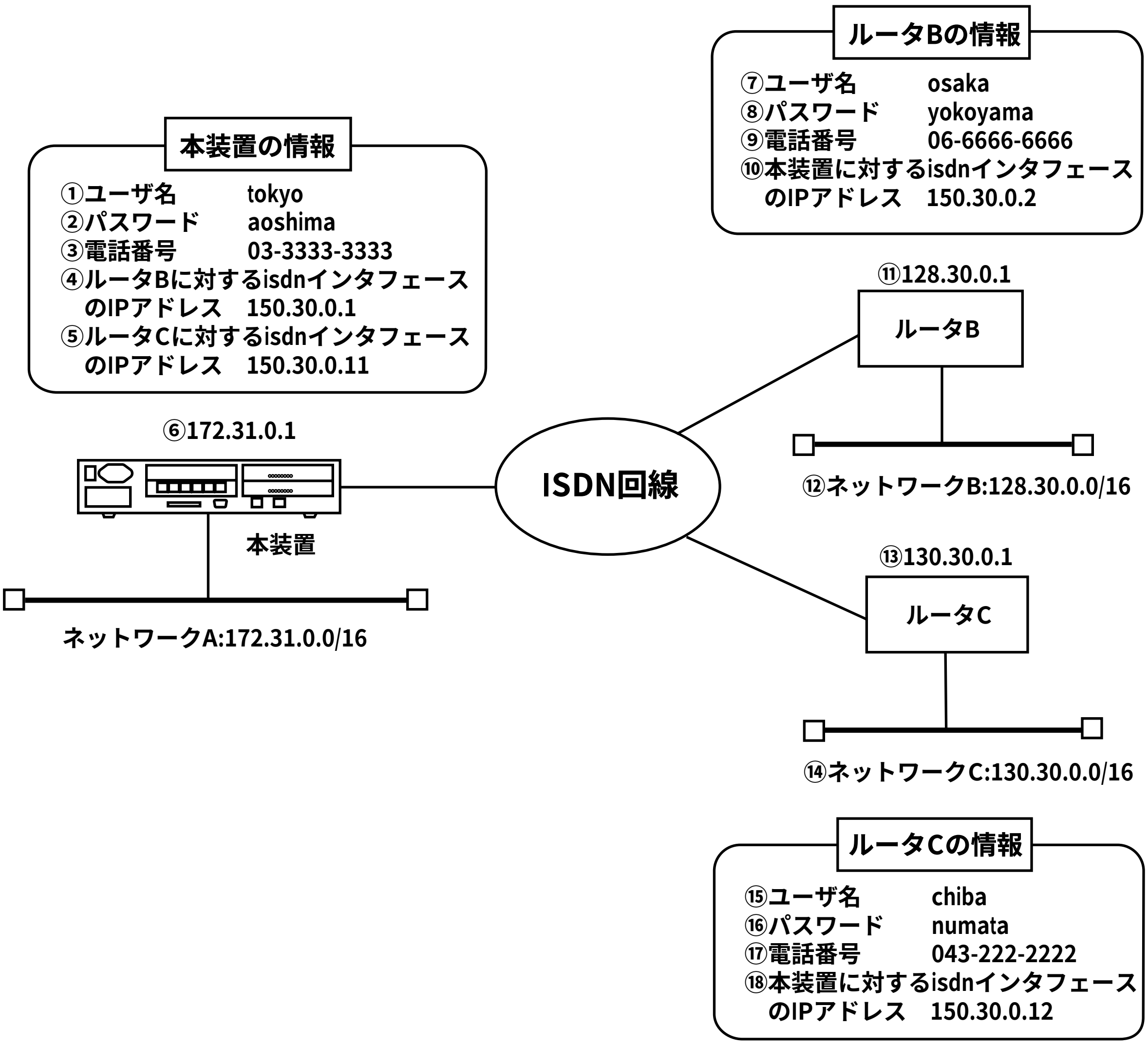
・この例は、ISDNインタフェースにIPアドレスを設定しない条件ですので、interfaceキーワードでunnumberedの設定を行っています。したがって自局IPアドレスは設定せず、また相手IPアドレスは相手ルータのIPアドレスを設定します。
またpppサブキーワードでPPP接続フェーズのIPCPのアドレスネゴシエーションの設定を行います。この設定は相手ルータの設定と合わせる必要があります。この例のように「ppp address on * *」と設定することによって、本装置は自身のIPアドレス（構成図の④）を送信し、また相手から送信されるIPアドレス（構成図⑧あるいは⑩）を受け入れます。

・さらに相手ネットワークへのルーティング情報を、destinationキーワードで設定します。この時経由するルータのIPアドレスには、interfaceキーワードで指定した相手IPアドレスを指定します。

（ここは空白のページです。）

4.2.3　ISDNインタフェースにIPアドレスを設定する場合の設定

［構成図］



その他の情報

⑲プロトコルはPPPを使用する。
⑳PPP認証はPAPを使用し、着信時には相手を認証し、発信時には相手に認証される。
㉑ネットワークB、ネットワークC宛のパケットにより自動発信する。
㉒アイドル監視（90秒）で自動切断する。
㉓PRI拡張ボードのポート1からポート6までISDN回線で使用する。

[本装置のusersファイルの設定]

```
%preset
      auth_request          pap
      auth_accept           none

%default
      auth_request          none
      auth_accept           pap
      local_name            tokyo
      local_passwd          aoshima
      connect_on_demand     on
      idle_timeout          120

%user
      remote_name           osaka
      remote_passwd         yokoyama
      remote_tel            06-6666-6666

      interface  isdn0/150.30.0.1  150.30.0.2  numbered
             ppp  address  on       *     *
      destination  128.30.0.0/16    via  150.30.0.2 2


%user
      remote_name           chiba
      remote_passwd         numata
      remote_tel            043-222-2222

      interface  isdn0/150.30.0.11 150.30.0.12  numbered
             ppp  address  on       *     *
      destination  130.30.0.0/16   via  150.30.0.12  2
```

[構成図の情報との対応]

<着信時の設定>
⑳PPP認証方式（着信）

<ルータB／ルータC共通の設定>
⑳PPP認証方式（発信）

①自局ユーザ名
㉑自局パスワード
㉒自動発信
①アイドル監視時間

<ルータBに対する設定>
⑦ユーザ名
⑧パスワード
⑨電話番号

④⑩論理インタフェースの設定

⑫ルーティング情報の設定

<ルータCに対する設定>
⑮ユーザ名
⑯パスワード
⑰電話番号

⑤⑱論理インタフェースの設定

⑭ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

⑥本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
       %port  1
              line_type isdn
       %port  2
              line_type isdn
       %port  3
              line_type isdn
       %port  4
              line_type isdn
       %port  5
              line_type isdn
       %port  6
              line_type isdn
```

[構成図の情報との対応]

㉓拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

［解　説］

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。この設定は全接続相手に共通になります。

・この例では、構成図の⑳の情報から、着信時にはPAPで相手を認証し、相手からの認証はされない設定をしています。

<usersファイル：ルータB／ルータC共通の設定>

・各接続相手に共通な設定は、%default分類キーワードに設定することによって、各接続相手ごとに設定する必要がなくなります。ここに設定されているキーワードは、<ルータBに対する設定>、<ルータCに対する設定>にそれぞれ記述してもかまいません。

・この例では、共通な設定項目として、

構成図の情報⑳：発信時には本装置からは認証を要求せず、相手からPAP認証要求を受け入れる。

構成図の情報㉑：自動発信する。

構成図の情報㉒：アイドル監視を90秒にする。

構成図の情報①、②：相手からPAP認証される場合の自局ユーザ名、パスワードなどを設定しています。

<usersファイル：ルータBに対する設定>
<usersファイル：ルータCに対する設定>

・各接続相手の条件は%user分類キーワードで設定します。

・この例では、まずPAPでPPP認証する場合のユーザ名、パスワードを設定しています。本装置は着信時に%presetキーワードに設定されているPAPによる認証を相手に要求し、相手から送られてくるユーザ名を元にusersファイルを検索し、ルータBあるいはルータCの%userエントリを特定します。

・%user分類キーワードには、接続相手ごとに論理インタフェースの設定、ルーティング情報の設定を行います。この情報をもとに、接続時に接続相手との間のデータ転送のためのルーティングテーブルを作成し、IPパケットのフォワーディングが可能になります。

・この例は、ISDNインタフェースにIPアドレスを設定する条件ですので、interfaceキーワードでnumberedの設定を行っています。したがってルータBに対しては、構成図の情報④から、ルータBに対する自局IPアドレスを「isdn0／150.30.0.1」に設定します。また相手IPアドレスは情報⑩から「150.30.0.2 」に設定します。この場合、ルータBのIPアドレスは使用しません。
ルータCも同様に設定します。

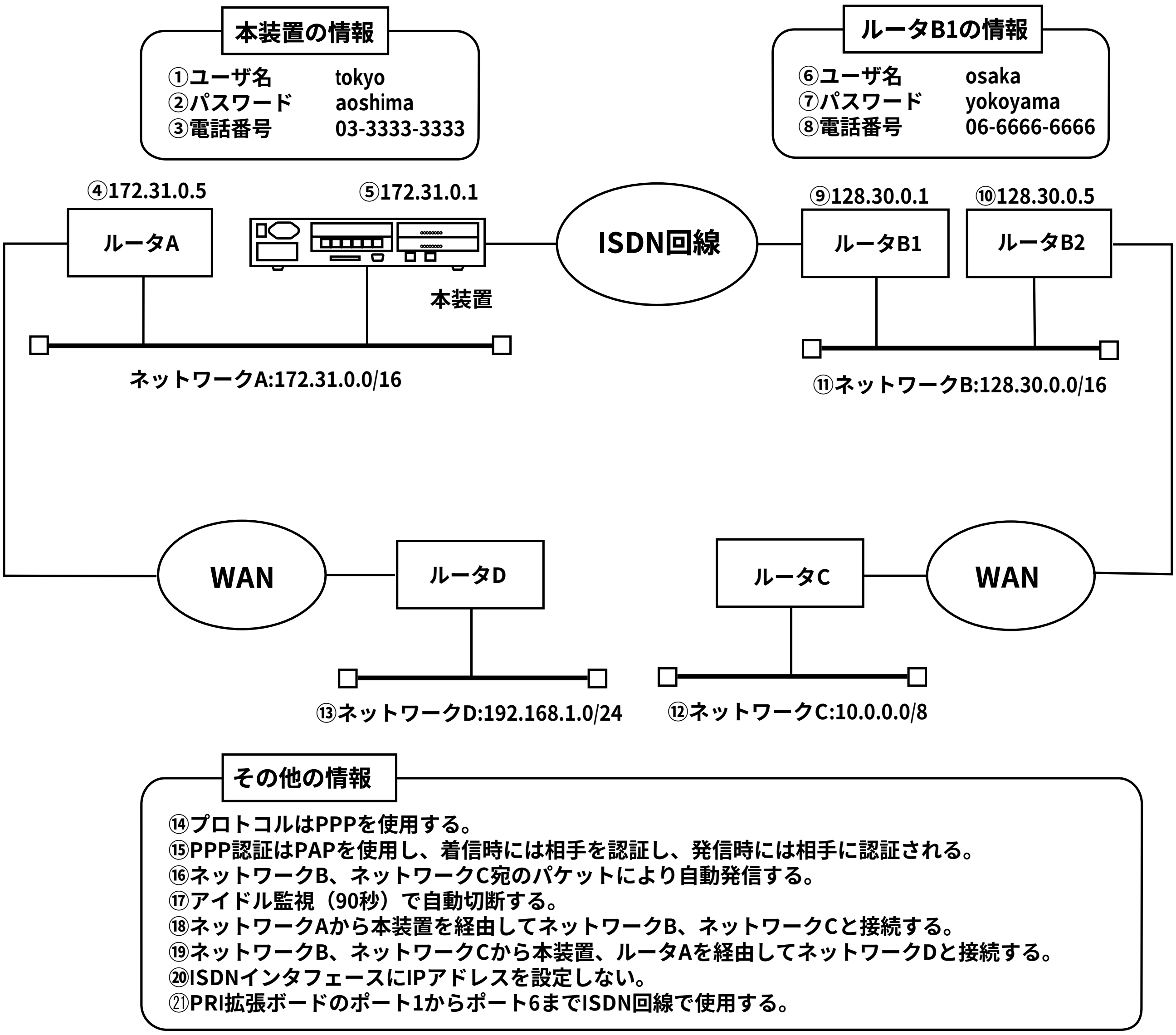
・pppサブキーワードでPPP接続フェーズのIPCPのアドレスネゴシエーションの設定を行います。この設定は相手ルータの設定と合わせる必要があります。この例のように「ppp　address on ＊ *」と設定することによって、ルータBに対しては、本装置は自身のIPアドレス（構成図の情報④）を送信し、また相手から送信されるIPアドレス（構成図の情報⑩）を受け入れます。

・さらに相手ネットワークへのルーティング情報を、destinationキーワードで設定します。この時経由するルータのIPアドレスには、interfaceキーワードで指定した相手IPアドレスを指定します。したがってルータBに対しては構成図の情報⑩を指定します。

（ここは空白のページです。）

4.2.4　複数のネットワークを経由する場合の設定

［構成図］



[本装置のusersファイルの設定]

```
%preset
      auth_request          pap
      auth_accept           none

%user
      remote_name           osaka
      remote_passwd         yokoyama
      local_name            tokyo
      local_passwd          aoshima
      auth_request          none
      auth_accept           pap
      remote_tel            06-6666-6666
      connect_on_demand     on
      idle_timeout          90

      interface  isdn0      128.30.0.1    unnumbered
             ppp  address  on      *      *

      destination  128.30.0.0/16  via  128.30.0.1     2
      destination  10.0.0.0/8     via  128.30.0.1     3
```

[構成図の情報との対応]

<着信時の設定>
⑮PPP認証方式（着信）

<ルータB1に対する設定>
⑥ユーザ名
⑦パスワード
①自局ユーザ名
②自局パスワード
⑮PPP認証方式(発信)

⑧電話番号
⑯自動発信
⑰アイドル監視時間

⑨⑳論理インタフェースの設定

⑪⑫ルーティング情報の設定

[本装置のgatewaysファイルの設定]

```
destination  192.168.1.0/24 via 172.31.0.5    2
```

[構成図の情報との対応]

⑬ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置ホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1 ns4200
```

[構成図の情報との対応]

⑤本装置ホスト名に対応するIPアドレスの設定

[本装置のboardsファイルの設定]

```
%board 1
       %port  1
              line_type isdn
       %port  2
              line_type isdn
       %port  3
              line_type isdn
       %port  4
              line_type isdn
       %port  5
              line_type isdn
       %port  6
              line_type isdn
```

[構成図の情報との対応]

㉑拡張ボードスロット1の拡張ボードの設定
（ポート1からポート6をISDN回線で使用する）

[本装置のinterfaceファイルの設定]

```
interface en0 */* numbered
```

[構成図の情報との対応]

LAN1ポート(en0)に関する設定
（LAN2ポートは使用しない）

［解　説］

<usersファイル：着信時の設定>

・着信の条件は%preset分類キーワードで設定します。

・この例では、構成図の⑮の情報から、着信時にはPAPで相手を認証し、相手からの認証はされない設定をしています。

<usersファイル：ルータB1に対する設定>

・接続相手の条件は%user分類キーワードで設定します。

構成図の情報①、②：相手からPAP認証される場合の自局ユーザ名、パスワード
構成図の情報⑮：発信時には本装置からは認証を要求せず、相手からPAP認証要求を受け入れる。
構成図の情報⑧：発信時の相手電話番号
構成図の情報⑯：自動発信する。
構成図の情報⑰：アイドル監視を90秒にする。

などをまず設定しています。

・さらに%user分類キーワードには、接続相手ごとに論理インタフェースの設定、ルーティング情報の設定を行います。この情報をもとに、接続時に接続相手との間のデータ転送のためのルーティングテーブルを作成し、IPパケットのフォワーディングが可能になります。

・この例は、ISDNインタフェースにIPアドレスを設定しない条件（構成図の情報⑳）ですので、interfaceキーワードでunnumberedの設定を行っています。したがって自局IPアドレスは設定せず、また相手IPアドレスは相手ルータのIPアドレスを設定します。
またpppサブキーワードでPPP接続フェーズのIPCPのアドレスネゴシエーションの設定を行います。この設定は相手ルータの設定と合わせる必要があります。この例のように「ppp address on * *」と設定することによって、本装置は自身のIPアドレス（構成図の⑤）を送信し、また相手から送信されるIPアドレス（構成図⑨）を受け入れます。

・さらに相手ネットワークへのルーティング情報を、destinationキーワードで設定します。この時経由するルータのIPアドレスには、interfaceキーワードで指定した相手IPアドレスを指定します。この例では、ルータＢ１経由でネットワークBとネットワークCに接続するので、それぞれに対してdestinationキーワードで設定します。

<gatewaysファイルの設定>

・LAN経由のスタティックなルーティング情報は、gatewaysファイルに設定します。

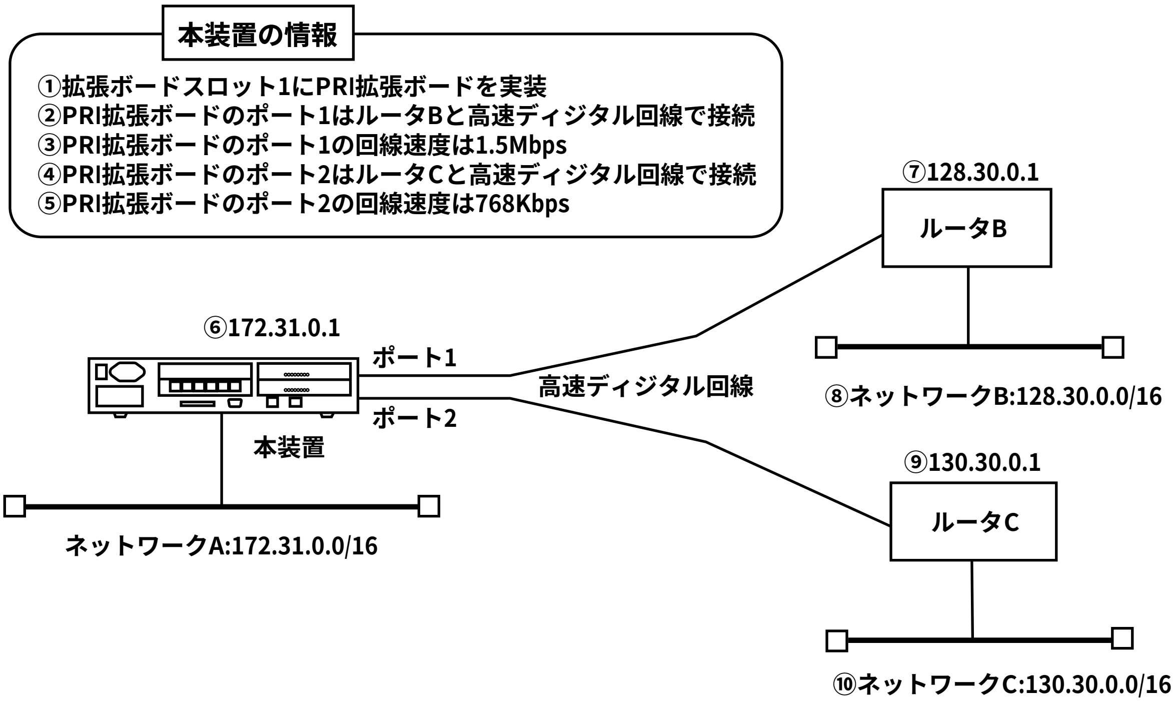
・この例では、構成図の情報⑲により、ルータAを経由してネットワークDにルーティングできるようにdestinationキーワードで設定します。

（ここは空白のページです。）

4.3　高速ディジタル回線経由でネットワーク型接続を行う場合の基本的な設定

4.3.1　高速ディジタル回線インタフェースにIPアドレスを設定しない場合の設定

［構成図］



[本装置のboardsファイルの設定]

```
%board 1
   %port 1
       line_type     hsd
       %channel      1
          slots      1-24


   %port 2
       line_type     hsd
       %channel      1
          slots      1-12
```

[構成図の情報との対応]

<①拡張ボードスロット1の拡張ボード設定>
<②ポート1の設定>
回線種別：高速ディジタル回線
<論理チャネル1の設定>
③回線速度を使用するタイムスロットで指定：1.5Mbps

<④ポート2の設定>
回線種別：高速ディジタル回線
<論理チャネル1の設定>
⑤回線速度を使用するタイムスロットで指定：768Kbps

[本装置のinterfaceファイルの設定]

```
interface en0        */*            numbered


interface hsd1       128.30.0.1     unnumbered
      channel 1/1/1


interface hsd2       130.30.0.1     unnumbered
      channel 1/2/1
```

[構成図の情報との対応]

⑥論理インタフェースen0(LAN1ポート)の設定(LAN2ポートは使用しない)

⑦論理インタフェースhsd1の設定
hsd1に対応付ける論理チャネルの設定:拡張ボードスロット1/ポート1/論理チャネル1

⑨論理インタフェースhsd2の設定
hsd2に対応付ける論理チャネルの設定:拡張ボードスロット1/ポート2/論理チャネル1

[本装置のgatewaysファイルの設定]

```
destination  128.30.0.0/16  via  128.30.0.1  2
destination  130.30.0.0/16  via  130.30.0.1  2
```

[構成図の情報との対応]

⑧ルーティング情報の設定
⑩ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置のホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1   ns4200
```

[構成図の情報との対応]

⑥本装置ホスト名に対応するIPアドレスの設定

［解　説］

<boardsファイルの設定>

・拡張ボードスロット1のPRI拡張ボードに対する設定をします。
・PRI拡張ボードのポート1とポート2を用いてルータBとルータCにそれぞれ接続します。
・ポート1のタイムスロット1～24を論理チャネル1として使用します。回線速度は、64Kbps×24タイムスロット = 1.5Mbpsとなります。この論理チャネルは、拡張ボードスロット番号、ポート番号とともにinterfaceファイルの論理インタフェースの設定時に使用します。
・ポート2のタイムスロット1～12を論理チャネル1として使用します。回線速度は、64Kbps×12タイムスロット= 768Kbpsとなります。この論理チャネルは、拡張ボードスロット番号、ポート番号とともにinterfaceファイルの論理インタフェースの設定時に使用します。

<interfaceファイルの設定>

・LAN1ポートに対応する論理インタフェースen0を設定します。numberdで自局IPアドレスを省略していますので、hostnameファイルに記述されたホスト名に対応するIPアドレスが使用されます。相手IPアドレスが「*/*」に設定されていますので、自局IPアドレスのネットワークアドレスとネットマスクが使用されます。なお、この例では、LAN2ポートは使用しません。
・この例では、hsdインタフェースにIPアドレスを設定しない条件ですので、interfaceキーワードでunnumberedの設定を行っています。したがって、自局IPアドレスを指定しないので「hsd1」のみで設定します。また相手IPアドレスは構成図の情報⑦から相手ルータBのIPアドレス「128.30.0.1」に設定します。
ルータCも同様に設定します。
・論理インタフェースhsd1に、boardsファイルに設定した拡張ボードスロット番号1、ポート番号1、論理チャネル番号1を関連付けます。
・論理インタフェースhsd2に、boardsファイルに設定した拡張ボードスロット番号1、ポート番号2、論理チャネル番号1を関連付けます。

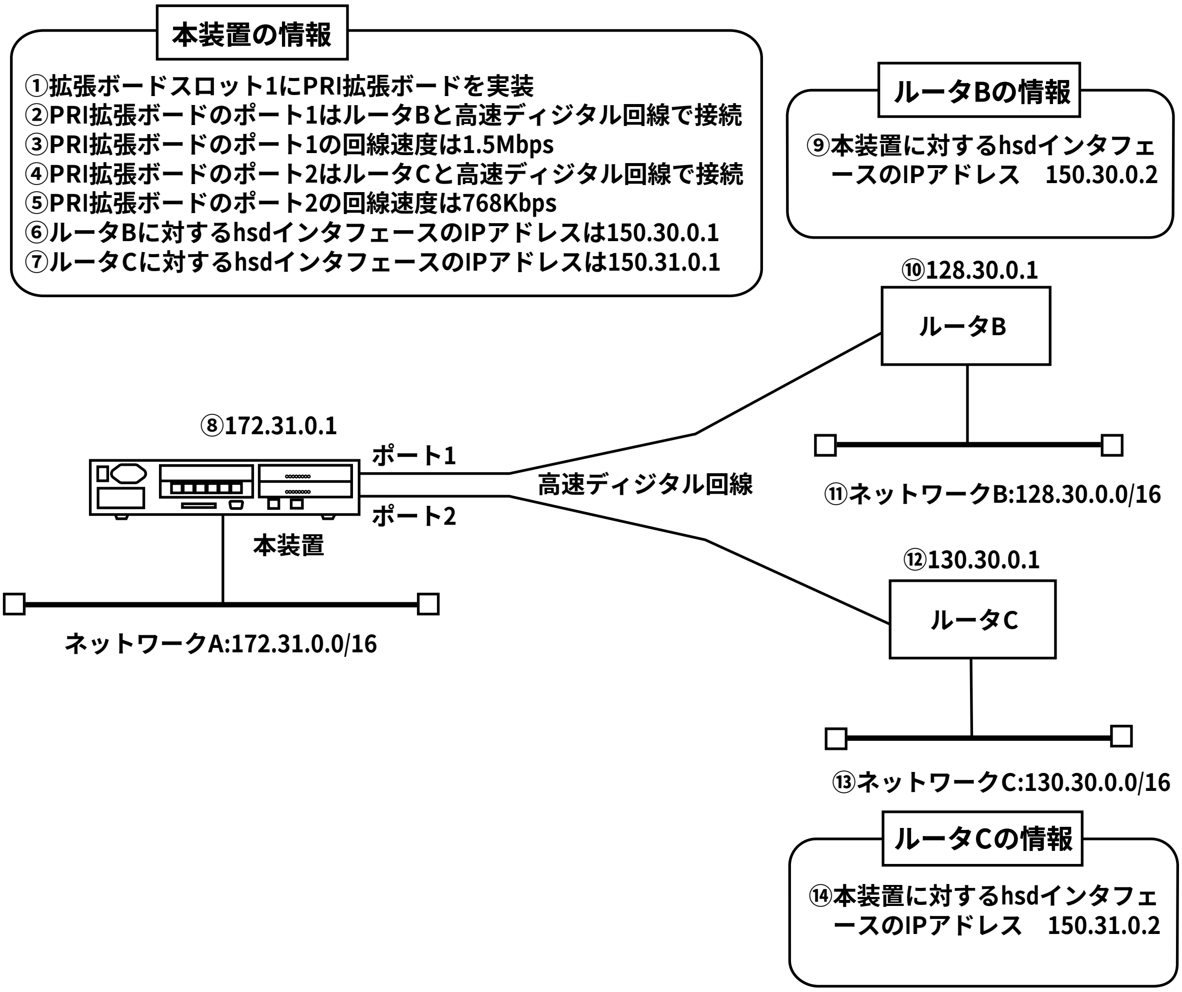
<gatewaysファイルの設定>

・相手ネットワークへのルーティング情報を、destinationキーワードで設定します。このとき、経由するルータのIPアドレスには、interfaceファイルのinterfaceキーワードで指定した相手IPアドレスを指定します。したがって、ルータBに対しては構成図の情報⑦を指定します。
ルータCも同様に設定します。

（ここは空白のページです。）

4.3.2　高速ディジタル回線インタフェースにIPアドレスを設定する場合の設定

［構成図］



[本装置のboardsファイルの設定]

```
%board 1
    %port 1
        line_type   hsd
        %channel    1
           slots    1-24


    %port 2
        line_type   hsd
        %channel    1
           slots    1-12
```

[構成図の情報との対応]

<①拡張ボードスロット1の拡張ボード設定>
<②ポート1の設定>
回線種別：高速ディジタル回線
<論理チャネル1の設定>
③回線速度を使用するタイムスロットで指定：1.5Mbps

<④ポート2の設定>
回線種別：高速ディジタル回線
<論理チャネル1の設定>
⑤回線速度を使用するタイムスロットで指定：768Kbps

[本装置のinterfaceファイルの設定]

```
interface en0              */*       numbered


interface hsd1/150.30.0.1 150.30.0.2 numbered
      channel 1/1/1


interface hsd2/150.31.0.1 150.31.0.2 numbered
      channel 1/2/1
```

[構成図の情報との対応]

⑧論理インタフェースen0(LAN1ポート)の設定(LAN2ポートは使用しない)

⑥⑨論理インタフェースhsd1の設定
hsd1に対応付ける論理チャネルの設定:拡張ボードスロット1/ポート1/論理チャネル1

⑦⑭論理インタフェースhsd2の設定
hsd2に対応付ける論理チャネルの設定:拡張ボードスロット1/ポート2/論理チャネル1

[本装置のgatewaysファイルの設定]

```
destination  128.30.0.0/16  via  150.30.0.2  2
destination  130.30.0.0/16  via  150.31.0.2  2
```

[構成図の情報との対応]

⑪ルーティング情報の設定
⑬ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置のホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1   ns4200
```

[構成図の情報との対応]

⑧本装置ホスト名に対応するIPアドレスの設定

［解　説］

<boardsファイルの設定>

・拡張ボードスロット1のPRI拡張ボードに対する設定をします。
・PRI拡張ボードのポート1とポート2を用いてルータBとルータCにそれぞれ接続します。
・ポート1のタイムスロット1〜24を論理チャネル1として使用します。回線速度は、64Kbps×24タイムスロット = 1.5Mbpsとなります。この論理チャネルは、拡張ボードスロット番号、ポート番号とともにinterfaceファイルの論理インタフェースの設定時に使用します。
・ポート2のタイムスロット1〜12を論理チャネル1として使用します。回線速度は、64Kbps×12タイムスロット = 768Kbpsとなります。この論理チャネルは、拡張ボードスロット番号、ポート番号とともにinterfaceファイルの論理インタフェースの設定時に使用します。

<interfaceファイルの設定>

・LAN1ポートに対応する論理インタフェースen0を設定します。numberdで自局IPアドレスを省略していますので、hostnameファイルに記述されたホスト名に対応するIPアドレスが使用されます。相手IPアドレスが「*/*」に設定されていますので、自局IPアドレスのネットワークアドレスとネットマスクが使用されます。なお、この例では、LAN2ポートは使用しません。
・この例では、hsdインタフェースにIPアドレスを設定する条件ですので、interfaceキーワードでnumberedの設定を行っています。したがって、ルータBに対しては、構成図の情報⑥から、ルータBに対する自局IPアドレスを「hsd1/150.30.0.1」に設定します。また相手IPアドレスは情報⑨から「150.30.0.2」に設定します。この場合、ルータBのIPアドレスは使用しません。
ルータCも同様に設定します。
・論理インタフェースhsd1に、boardsファイルに設定した拡張ボードスロット番号1、ポート番号1、論理チャネル番号1を関連付けます。
・論理インタフェースhsd2に、boardsファイルに設定した拡張ボードスロット番号1、ポート番号2、論理チャネル番号1を関連付けます。

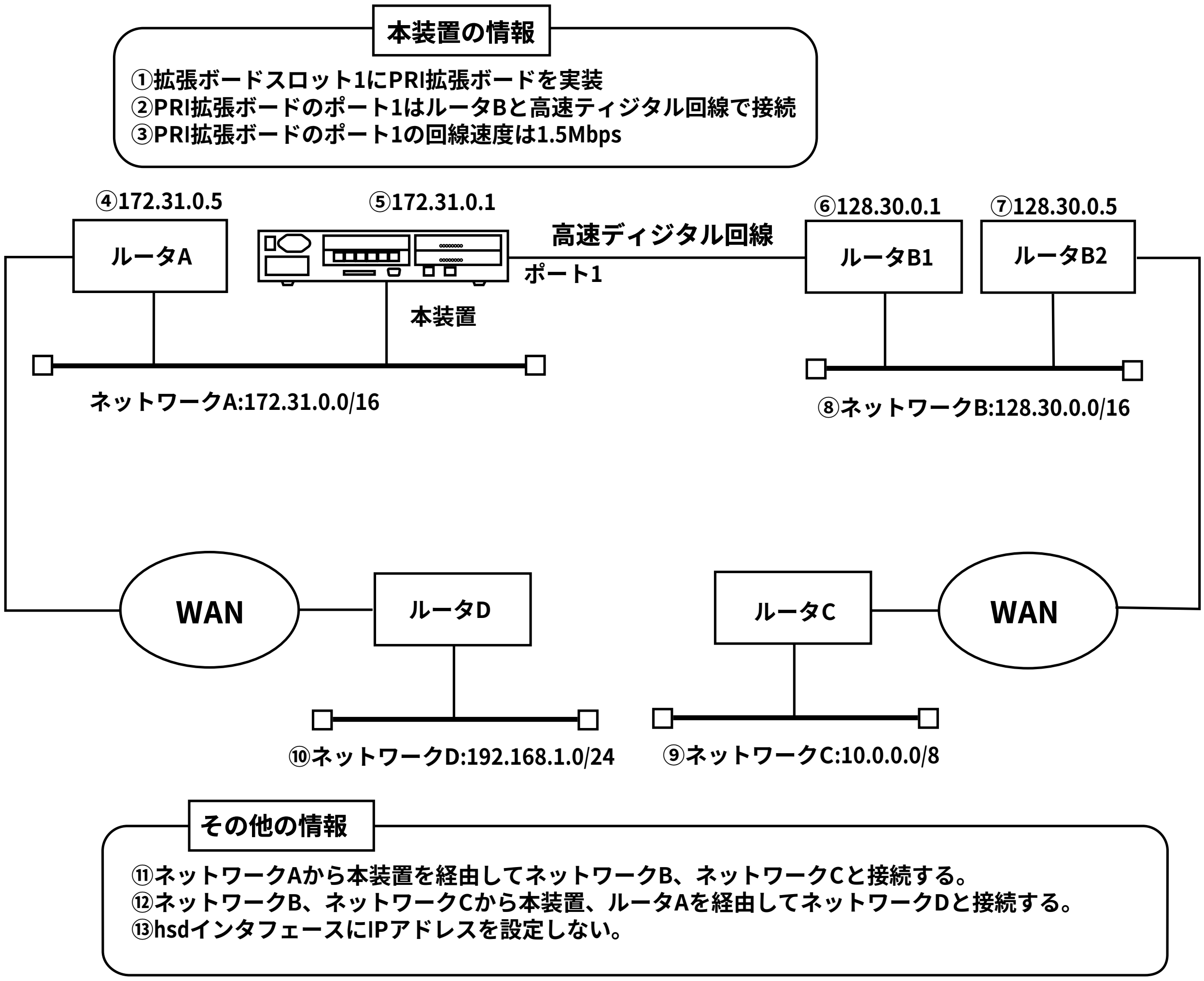
<gatewaysファイルの設定>

・相手ネットワークへのルーティング情報を、destinationキーワードで設定します。このとき、経由するルータのIPアドレスには、interfaceファイルのinterfaceキーワードで指定した相手IPアドレスを指定します。したがって、ルータBに対しては構成図の情報⑨を指定します。
ルータCも同様に設定します。

（ここは空白のページです。）

4.3.3　複数のネットワークを経由する場合の設定

［構成図］



[本装置のboardsファイルの設定]

```
%board 1
    %port 1
        line_type   hsd
        %channel    1
           slots    1-24
```

[構成図の情報との対応]

<①拡張ボードスロット1の拡張ボード設定>
<②ポート1の設定>
回線種別：高速ディジタル回線
<論理チャネル1の設定>
③回線速度を使用するタイムスロットで指定：1.5Mbps

[本装置のinterfaceファイルの設定]

```
interface en0       */*        numbered


interface hsd1   128.30.0.1   unnumbered
      channel 1/1/1
```

[構成図の情報との対応]

⑤論理インタフェースen0(LAN1ポート)の設定(LAN2ポートは使用しない)

⑥論理インタフェースhsd1の設定
hsd1に対応付ける論理チャネルの設定：拡張ボードスロット1/ポート1/論理チャネル1

[本装置のgatewaysファイルの設定]

```
destination  128.30.0.0/16  via  128.30.0.1  2
destination  10.0.0.0/8     via  128.30.0.1  3
destination  192.168.1.0/24 via  172.31.0.5  2
```

[構成図の情報との対応]

⑥⑧ルーティング情報の設定
⑥⑨ルーティング情報の設定
④⑩ルーティング情報の設定

[本装置のhostnameファイルの設定]

```
ns4200
```

[構成図の情報との対応]

本装置のホスト名の設定

[本装置のhostsファイルの設定]

```
172.31.0.1   ns4200
```

[構成図の情報との対応]

⑤本装置ホスト名に対応するIPアドレスの設定

［解　説］

<boardsファイルの設定>

・拡張ボードスロット1のPRI拡張ボードに対する設定をします。
・PRI拡張ボードのポート1を用いてルータBに接続します。
・ポート1のタイムスロット1～24を論理チャネル1として使用します。回線速度は、64Kbps×24タイムスロット= 1.5Mbpsとなります。
　この論理チャネルは、拡張ボードスロット番号、ポート番号とともにinterfaceファイルの論理インタフェースの設定時に使用します。

<interfaceファイルの設定>

・LAN1ポートに対応する論理インタフェースen0を設定します。numberdで自局IPアドレスを省略していますので、hostnameファイルに記述されたホスト名に対応するIPアドレスが使用されます。相手IPアドレスが「*/*」に設定されていますので、自局IPアドレスのネットワークアドレスとネットマスクが使用されます。なお、この例では、LAN2ポートは使用しません。
・この例では、hsdインタフェースにIPアドレスを設定しない条件ですので、interfaceキーワードでunnumberedの設定を行っています。したがって、自局IPアドレスを指定しないので「hsd1」のみで設定します。また相手IPアドレスは構成図の情報⑥から「128.30.0.1」に設定します。
・論理インタフェースhsd1に、boardsファイルに設定した拡張ボードスロット番号1、ポート番号1、論理チャネル番号1を関連付けます。

<gatewaysファイルの設定>

・相手ネットワークへのルーティング情報を、destinationキーワードで設定します。このとき、経由するルータのIPアドレスには、interfaceファイルのinterfaceキーワードで指定した相手IPアドレスを指定します。この例では、ルータB経由でネットワークBとネットワークCに接続するので、それぞれに対してdestinationキーワードで設定します。
・また、ルータAを経由してネットワークDに接続するルーティング情報をdestinationキーワードで設定します。

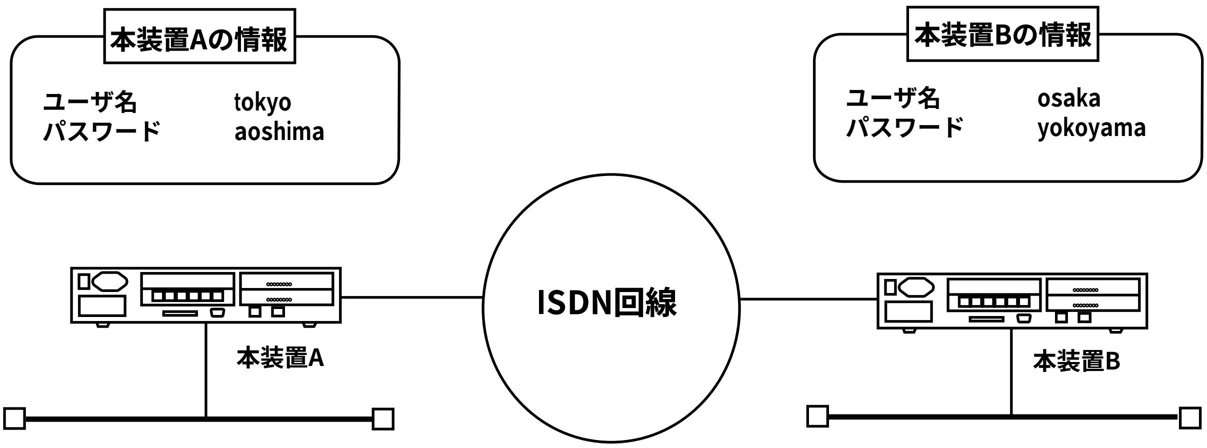
（ここは空白のページです。）

4.4 ISDN接続の詳細機能の設定

4.4.1 PPP認証を使用する場合の設定

ここでは、PPP認証を行う場合の設定方法について説明します。設定例においては、PPP認証の設定部分のみについて記述しています。

(1) PAPによる片方向認証



[本装置Aのusersファイルの設定]

```
%preset

%user
        auth_request      none①
        auth_accept       pap②
        local_name        tokyo③
        local_passwd      aoshima④
```

[本装置Bのusersファイルの設定]

```
%preset
        auth_request          pap⑤
        auth_accept           none⑥

%user
        remote_name           tokyo⑦
        remote_passwd         aoshima⑧
```

[解　説]

・本装置Aが発信して相手 (本装置B) にPAPで認証される場合、本装置A側のusersファイルを次のように設定します。

① 要求する認証方式 (%userのauth_request) を認証なし (none) にします。
② 受け入れる認証方式 (%userのauth_accept) をpapにします。
③ 認証される自局のユーザ名 (%userのlocal_name) を指定します。
④ 認証される自局のパスワード (%userのlocal_passwd) を指定します。

・本装置Bが着信して相手 (本装置A) をPAPで認証する場合、本装置B側のusersファイルを次のように設定します。

⑤ 要求する認証方式 (%presetのauth_request) をpapにします。
⑥ 受け入れる認証方式 (%presetのauth_accept) を認証なし (none) にします。
⑦ 認証する相手のユーザ名 (%userのremote_name) を指定します。
⑧ 認証する相手のパスワード (%userのremote_passwd) を指定します。

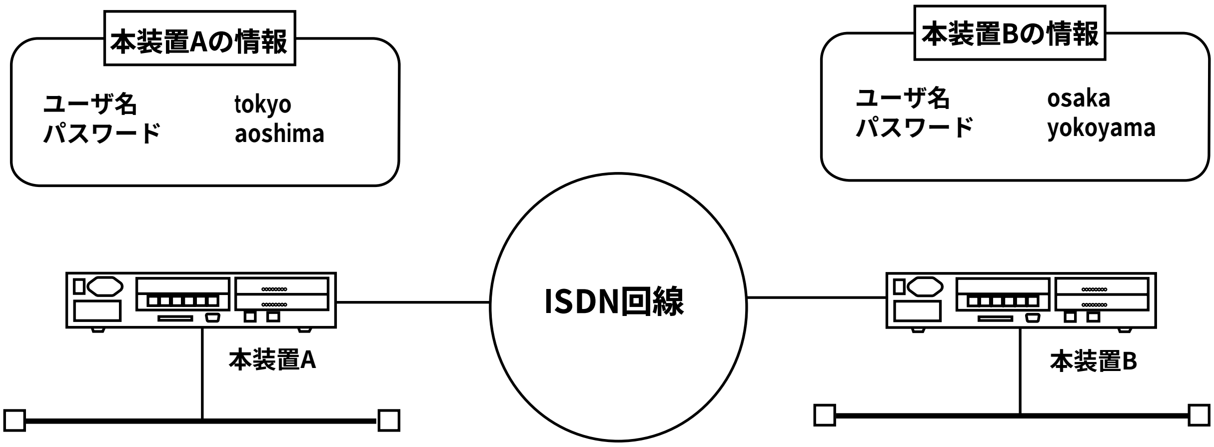
[参　考]

・本装置Aが発信したときは相手にPAPで認証され、かつ、着信したときは相手をPAPで認証する場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

```
%preset
      auth_request         pap
      auth_accept          none
%user
      auth_request         none
      auth_accept          pap
      remote_name          osaka
      remote_passwd        yokoyama
      local_name           tokyo
      local_passwd         aoshima
```

(2) PAPによる両方向認証



［本装置Aのusersファイルの設定］

```
%preset

%user
        auth_request      pap①
        auth_accept       pap②
        remote_name       osaka③
        remote_passwd     yokoyama④
        local_name        tokyo⑤
        local_passwd      aoshima⑥
```

［本装置Bのusersファイルの設定］

```
%preset
        auth_request      pap⑦
        auth_accept       pap⑧

%user
        remote_name       tokyo⑨
        remote_passwd     aoshima⑩
        local_name        osaka⑪
        local_passwd      yokoyama⑫
```

[解　説]

・本装置Aが発信して相手 (本装置B) にPAPで認証され、かつ、相手をPAPで認証する場合、本装置Aのusersファイルを次のように設定します。

① 要求する認証方式 (%userのauth_request) をpapにします。
② 受け入れる認証方式 (%userのauth_accept) をpapにします。
③ 認証する相手のユーザ名 (%userのremote_name) を指定します。
④ 認証する相手のパスワード (%userのremote_passwd) を指定します。
⑤ 認証される自局のユーザ名 (%userのlocal_name) を指定します。
⑥ 認証される自局のパスワード (%userのlocal_passwd) を指定します。

・本装置Bが着信して相手 (本装置A) をPAPで認証し、かつ、相手にPAPで認証される場合、本装置Bのusersファイルを次のように設定します。

⑦ 要求する認証方式 (%presetのauth_request) をpapにします。
⑧ 受け入れる認証方式 (%presetのauth_accept) をpapにします。
⑨ 認証する相手のユーザ名 (%userのremote_name) を指定します。
⑩ 認証する相手のパスワード (%userのremote_passwd) を指定します。
⑪ 認証される自局のユーザ名 (%userのlocal_name) を指定します。
⑫ 認証される自局のパスワード (%userのlocal_passwd) を指定します。

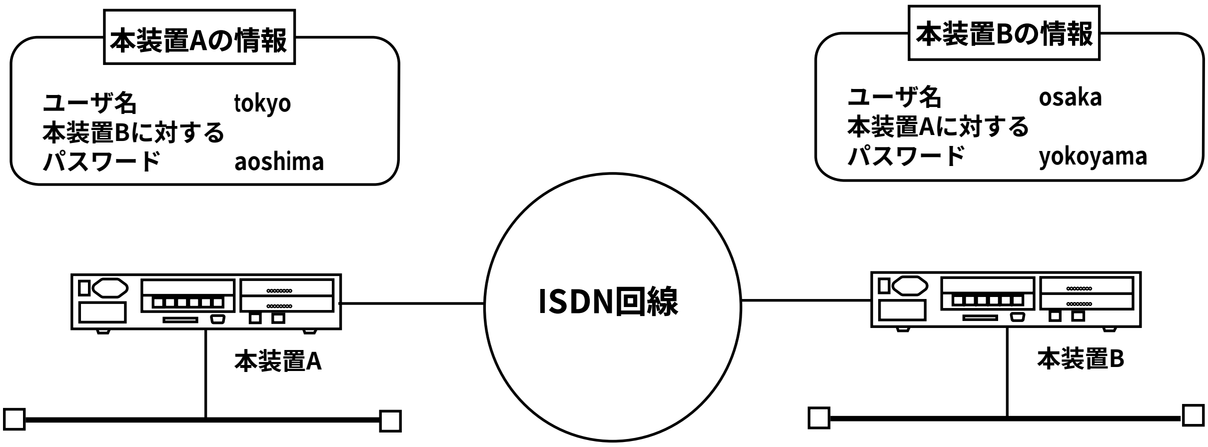
[参　考]

・本装置Aが発信したときも着信したときも、相手をPAPで認証し、かつ、相手にPAPで認証される場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

```
%preset
       auth_request         pap
       auth_accept          pap
%user
       auth_request         pap
       auth_accept          pap
       remote_name          osaka
       remote_passwd        yokoyama
       local_name           tokyo
       local_passwd         aoshima
```

(3) CHAPによる片方向認証



［本装置Aのusersファイルの設定］

```
%preset

%user
        auth_request     none①
        auth_accept      chap②
        local_name       tokyo③
        local_passwd     aoshima④
```

［本装置Bのusersファイルの設定］

```
%preset
        auth_request     chap⑤
        auth_accept      none⑥

%user
        remote_name      tokyo⑦
        remote_passwd    aoshima⑧
```

[解　説]

・本装置Aが発信して相手 (本装置B) にCHAPで認証される場合、本装置Aのusersファイルを次のように設定します。

① 要求する認証方式 (%userのauth_request) を認証なし (none) にします。
② 受け入れる認証方式 (%userのauth_accept) をchapにします。
③ 認証される自局のユーザ名 (%userのlocal_name) を指定します。
④ 認証される自局のパスワード (%userのlocal_passwd) を指定します。

・本装置Bが着信して相手 (本装置A) をCHAPで認証する場合、本装置Bのusersファイルを次のように設定します。

⑤ 要求する認証方式 (%presetのauth_request) をchapにします。
⑥ 受け入れる認証方式 (%presetのauth_accept) を認証なし (none) にします。
⑦ 認証する相手のユーザ名 (%userのremote_name) を指定します。
⑧ 認証する相手のパスワード (%userのremote_passwd) を指定します。

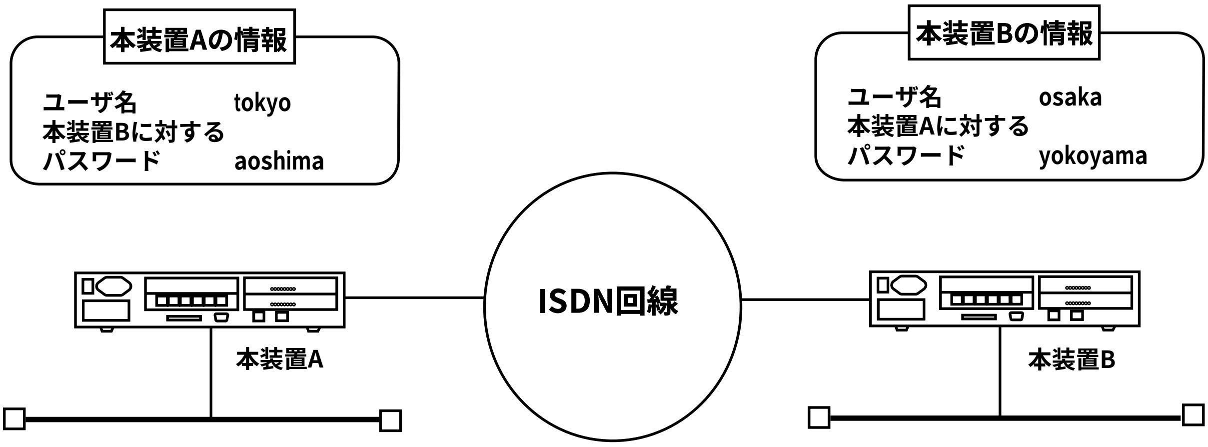
[参　考]

・本装置Aが発信したときは相手にCHAPで認証され、かつ、着信したときは相手をCHAPで認証する場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

```
%preset
       auth_request        chap
       auth_accept         none
%user
       auth_request        none
       auth_accept         chap
       remote_name         osaka
       remote_passwd       yokoyama
       local_name          tokyo
       local_passwd        aoshima
```

(4) CHAPによる両方向認証



[本装置Aのusersファイルの設定]

```
%preset

%user
        auth_request     chap①
        auth_accept      chap②
        remote_name      osaka③
        remote_passwd    yokoyama④
        local_name       tokyo⑤
        local_passwd     aoshima⑥
```

[本装置Bのusersファイルの設定]

```
%preset
        auth_request     chap⑦
        auth_accept      chap⑧

%user
        remote_name      tokyo⑨
        remote_passwd    aoshima⑩
        local_name       osaka⑪
        local_passwd     yokoyama⑫
```

[解　説]

・本装置Aが発信して相手（本装置B）にCHAPで認証され、かつ、相手をCHAPで認証する場合、本装置Aのusersファイルを次のように設定します。

① 要求する認証方式（%userのauth_request）をchapにします。
② 受け入れる認証方式（%userのauth_accept）をchapにします。
③ 認証する相手のユーザ名（%userのremote_name）を指定します。
④ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑤ 認証される自局のユーザ名（%userのlocal_name）を指定します。
⑥ 認証される自局のパスワード（%userのlocal_passwd）を指定します。

・本装置Bが着信して相手（本装置A）をCHAPで認証し、かつ、相手にCHAPで認証される場合、本装置Bのusereファイルを次のように設定します。

⑦ 要求する認証方式（%presetのauth_request）をchapにします。
⑧ 受け入れる認証方式（%presetのauth_accept）をchapにします。
⑨ 認証する相手のユーザ名（%userのremote_name）を指定します。
⑩ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑪ 認証される自局のユーザ名（%userのlocal_name）を指定します。
⑫ 認証される自局のパスワード（%userのlocal_passwd）を指定します。

[参　考]

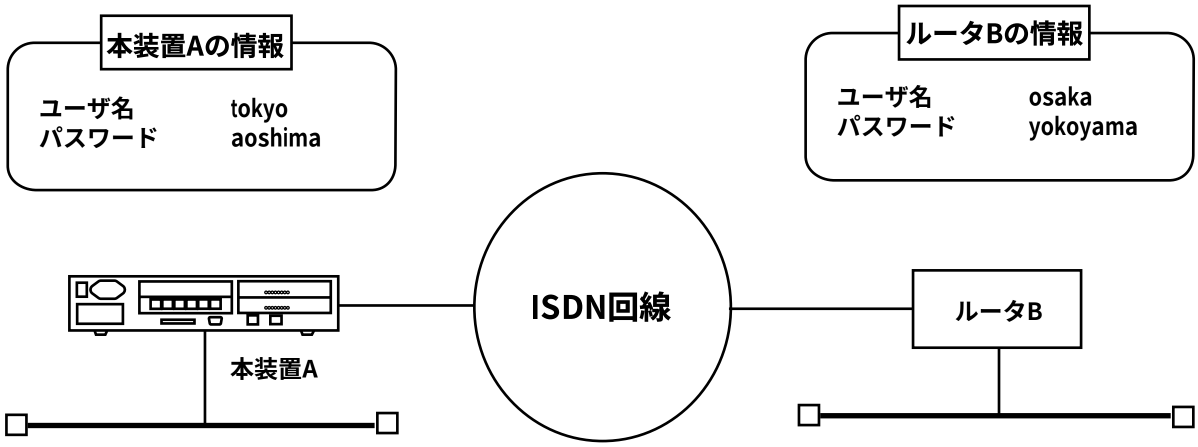
・本装置Aが発信したときも着信したときも、相手をCHAPで認証し、かつ、相手にCHAPで認証される場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

```
%preset
       auth_request         chap
       auth_accept          chap
%user
       auth_request         chap
       auth_accept          chap
       remote_name          osaka
       remote_passwd        yokoyama
       local_name           tokyo
       local_passwd         aoshima
```

(5) 着信時にCHAPあるいはPAPで認証する場合

端末型接続などにおいて、接続相手が受け入れる認証方式がCHAPかPAPかわからない場合には、以下の設定方法があります。この例では、ルータBが接続相手であり、ルータBから発信し、本装置Aが着信する場合に、ルータBが受け入れる認証方式がCHAPであるかPAPであるかがわからない場合を想定しています。



［本装置Aのusersファイルの設定］

```
%preset
       auth_request          either①
       auth_accept           none②
%user
       remote_name           osaka③
       remote_passwd         yokoyama④
```

［解　説］

・本装置Aが着信して相手（ルータB）をCHAPまたはPAPで認証する場合、本装置Aのusersファイルを次のように設定します。

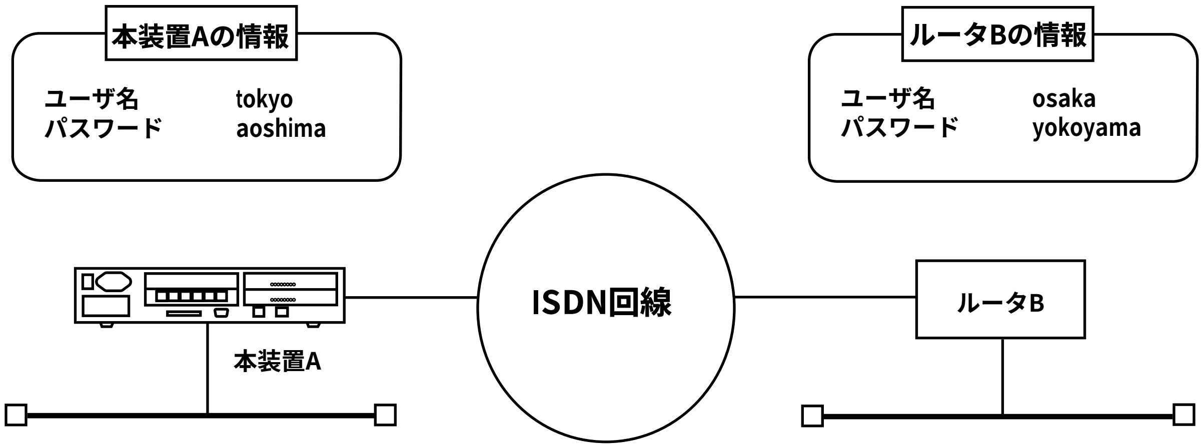
① 要求する認証方式（%presetのauth_request）をeitherにします。
② 受け入れる認証方式（%presetのauth_accept）をnoneにします。
③ 認証する相手のユーザ名（%userのremote_name）を指定します。
④ 認証する相手のパスワード（%userのremote_passwd）を指定します。

・auth_requestに「either」を指定した場合、本装置はまずCHAPを要求し、相手が受け入れた場合にはCHAPで認証します。もし相手がCHAPを受け入れない場合には、次にPAPを要求し、受け入れた場合にはPAPで認証します。相手がPAPも受け入れない場合には着信を拒否します。

注　意　　**本装置で両方向認証を行う場合には、相手に要求する認証方式と、受け入れる認証方式がPAPあるいはCHAPで一致している必要があります。したがって auth_requestに「either」を指定して両方向認証を行う場合には、注意が必要です。**

(6) 発信時にCHAPあるいはPAPで認証される場合

自局から発信し、接続相手から認証される場合に、接続相手から要求される認証方式がCHAPかPAPかわからない場合には、以下の設定方法があります。この例では、ルータBが接続相手であり、本装置Aから発信し、本装置Aは認証を要求しない。ルータBが着信する場合に、ルータBが要求してくる認証方式がCHAPであるかPAPであるかがわからない場合を想定しています。



［本装置Ａのusersファイルの設定］

```
%preset

%user
       auth_request         none①
       auth_accept          remote②
       local_name           tokyo③
       local_passwd         aoshima④
```

［解　説］

・本装置Aが発信して相手（ルータB）にCHAPまたはPAPで認証される場合、本装置Aのusersファイルを次のように設定します。

①要求する認証方式（%userのauth_request）を認証なし（none）にします。
②受け入れる認証方式（%userのauth_accept）を"相手先に合わせる"（remote）にします。
③認証される自局のユーザ名（%userのlocal_name）を指定します。
④認証される自局のパスワード（%userのlocal_passwd）を指定します。

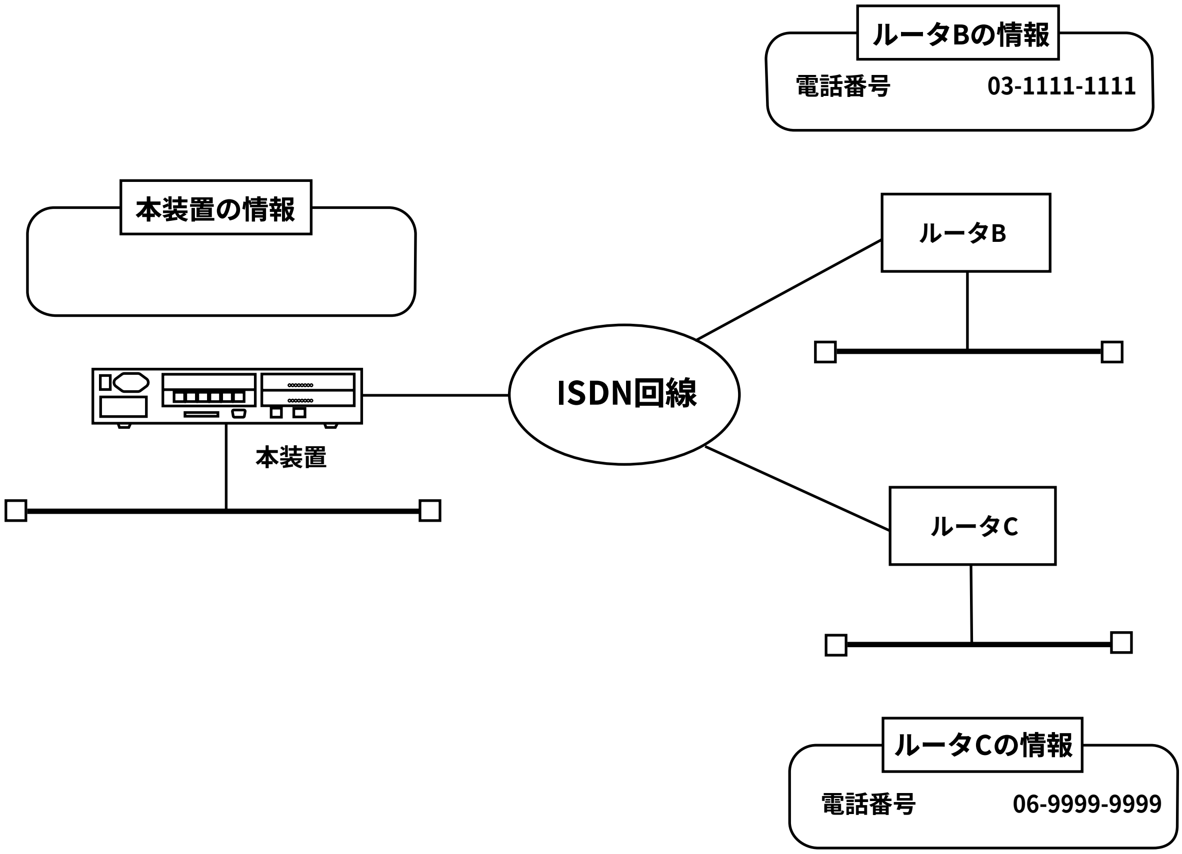
・ auth_acceptに「remote」を指定した場合、本装置は相手が要求する認証方式（CHAP、PAP）を受け入れます。もし認証要求がない場合には、認証されないで相手に接続することもできます。

注　意　　**本装置で両方向認証を行う場合には、相手に要求する認証方式と、受け入れる認証方式がPAPあるいはCHAPで一致している必要があります。したがってauth_acceptに「remote」を指定して両方向認証を行う場合には、注意が必要です。**

4.4.2　CLID認証を使用する場合の設定

ここでは、CLID認証に関するいくつかの設定について下図の構成を用いて説明します。なお設定例は、CLID認証に関連する部分のみを記述しています。

(1) ISDN着信時にすべての接続相手のCLID認証を行う場合



[本装置のusersファイルの設定]

```
%preset
       clid_auth            must

%user  # ルータBに対する設定
       remote_tel           03-1111-1111

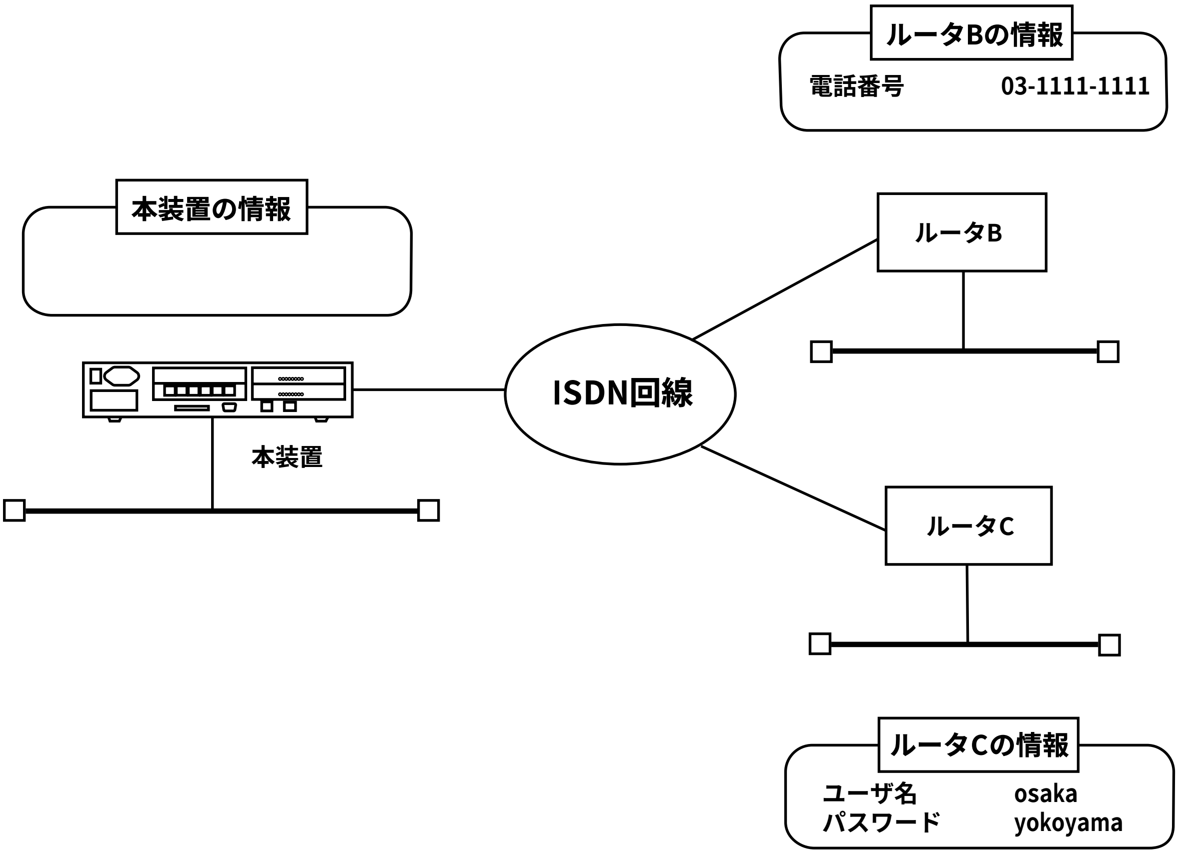
%user  # ルータCに対する設定
       remote_tel           06-9999-9999
```

[解　説]

・CLID認証（発信者電話番号による認証）を行う場合、%presetのclid_authをmustにします。この設定の場合、本装置はISDNからの着信を検出した時、usersファイルに登録されている%userエントリをチェックし、発信者電話番号と、remote_telあるいはaccept_telに設定されている電話番号を比較します。もし一致するremote_telあるいはaccept_telを含む %userエントリが見つからなかった場合には、着信を拒否します。

・この例では、ルータB、ルータCともに正しい電話番号が設定されていますので、ルータB、ルータCともにCLID認証が成功し、接続が許可されます。

(2) ISDN着信時にCLID認証に失敗しても着信を許可する場合



例えばネットワーク型接続の接続相手から着信した場合にはCLID認証を行い、端末型接続の接続相手から着信した場合には、CLID認証は行わずにPPP認証を行うような場合には、この設定方法が便利です。
この例では、ルータBからの着信時はCLID認証を行い、ルータCからの着信時はCLID認証を行わずにPPP認証を行うことを想定しています。

[本装置のusersファイルの設定]

```
%preset
        clid_auth            may
        auth_request         pap
        auth_accept          none

%user   # ルータBに対する設定
        remote_tel           03-1111-1111

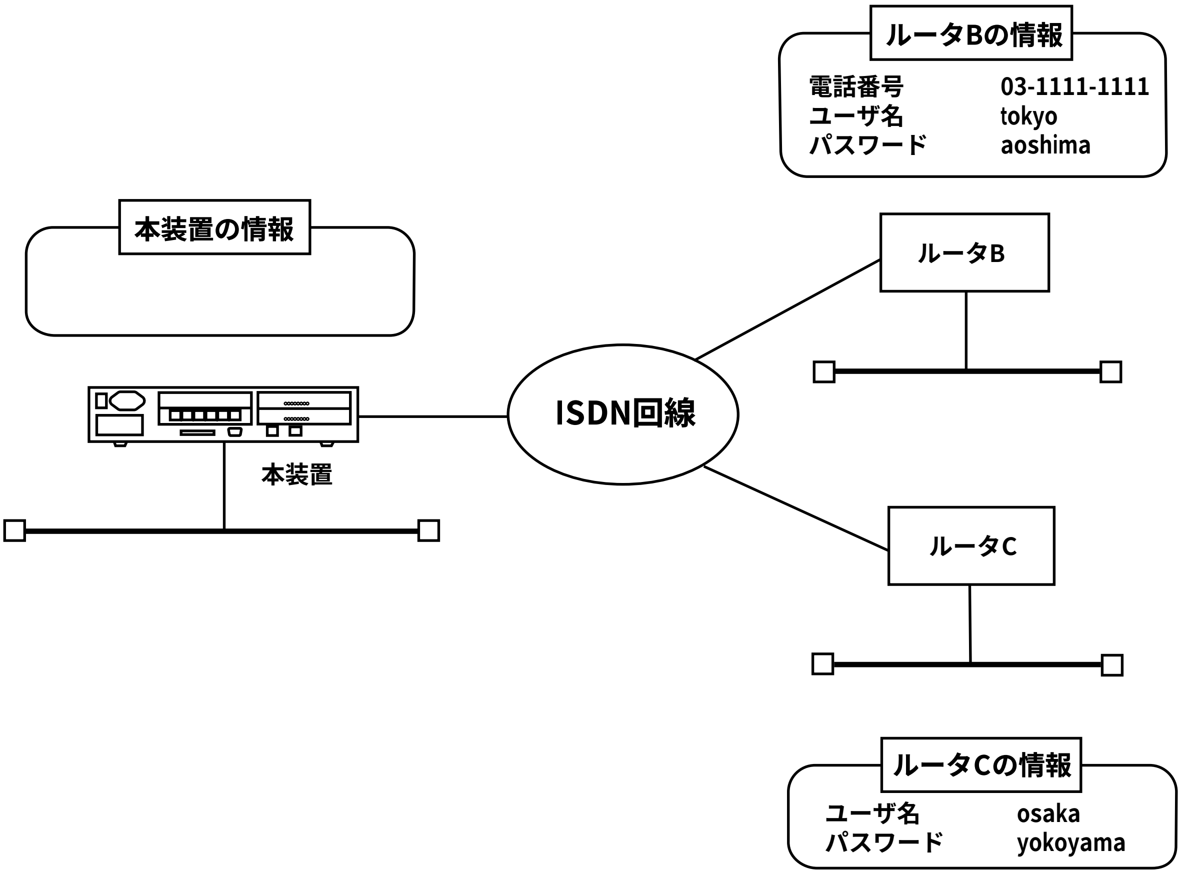
%user   # ルータCに対する設定
        remote_name          osaka
        remote_passwd        yokoyama
```

[解　説]

・CLID認証（発信者電話番号による認証）を行う場合、%presetのclid_authをmayにします。この設定の場合、本装置はISDNからの着信を検出した時、usersファイルに登録されている%userエントリをチェックし、発信者電話番号と、remote_telあるいはaccept_telに設定されている電話番号を比較します。もし一致するremote_telあるいはaccept_telを含む %userエントリが見つかった場合には、ISDNの着信を許可します。この時点で着信相手に対する %userエントリが特定できるため、その後PPP認証を行わなくても接続することができます。一方、一致するremote_telあるいはaccept_telを含む %userエントリが見つからなかった場合でも、ISDNの着信を許可します。ただしこの場合にはまだ着信相手の認証が行われていないため、その後PPP認証を行う必要があります。

・この例では、ルータBからの着信時には、ルータBに対する %userエントリにremote_telで電話番号が設定されているので、CLID認証で接続できます。
ルータCからの着信の場合、ルータCに対する %userエントリにremote_telが設定されていないため、CLID認証では失敗しますが、ISDNの着信は許可されます。その後 %presetのauth_requestの設定にしたがってPPP認証のPAPが実行されます。その際、ルータCに対する%userエントリにPAP認証の情報（remote_name、remote_passwd）が設定されていますので、PAPによるPPP認証が成功し、接続が許可されます。

(3) ISDN着信時にはCLID認証は行わず、PPP認証時にCLID認証を行う場合



この例では、ルータBは、PPP認証時にCLID認証を行い、ルータCはCLID認証は行わずPPP認証のみを行う場合を想定しています。

[本装置のusersファイルの設定]

```
%preset
        clid_auth               off
        auth_request            pap
        auth_accept             none

%user   # ルータBに対する設定
        remote_name             tokyo
        remote_passwd           aoshima
        clid_auth               must
        remote_tel              03-1111-1111

%user   # ルータCに対する設定
        remote_name             osaka
        remote_passwd           yokoyama
```

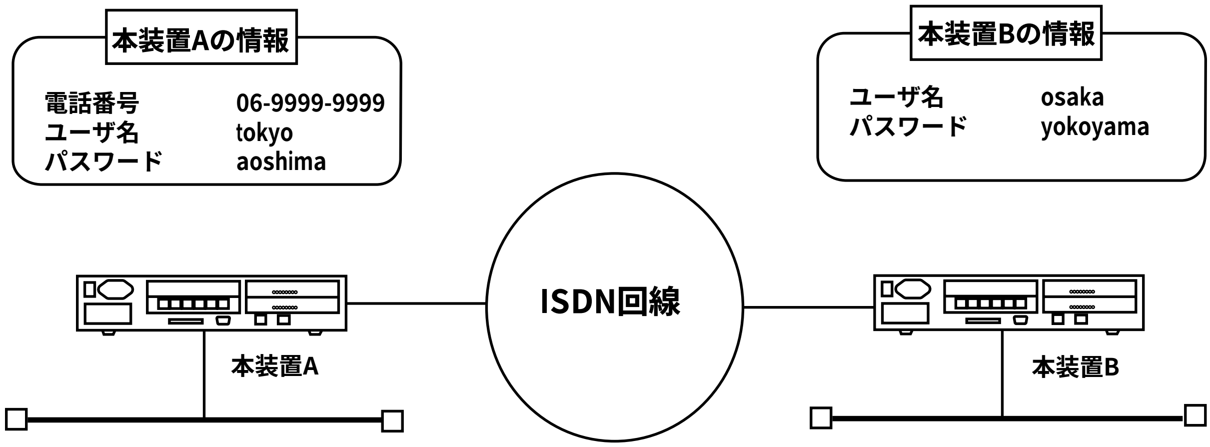
［解　説］

・CLID認証（発信者電話番号による認証）を行わない場合、%presetのclid_authをoffにします。この設定によりISDNの着信時にはCLID認証は行いません。このキーワードは「off」がデフォルト値ですから、設定を省略してもかまいません。
・%presetには、PPP認証の条件も設定します。
・ルータBの %userエントリでは、PPP認証の設定（remote_name、remote_passwd）の他に電話番号をチェックするためにclid_authをmustに設定し、remote_telにはルータBの電話番号を設定します。
この設定によって、PPP認証（PAP）を行った後さらに電話番号のチェックも行います。電話番号が一致していれば接続が認められますが、電話番号が一致していないと、PPP認証が成功していても接続は拒否されます。
・一方ルータCからの着信では、%userエントリにはclid_authが設定されていないので、PAPによるPPP認証のみ行われ、接続が許可されます。

4.4.3　CLID認証とPPP認証を併用する場合の設定

ここでは、CLID認証とPPP認証を併用する場合の設定方法について説明します。設定例においてはCLID認証とPPP認証の設定部分のみについて記述しています。

(1) CLID認証とPPP認証（PAP）による片方向認証の併用



[本装置Aのusersファイルの設定]

```
%preset


%user
        auth_request    none①
        auth_accept     pap②
        local_name      tokyo③
        local_passwd    aoshima④
```

[本装置Bのusersファイルの設定]

```
%preset
        clid_auth       must⑤
%user
        auth_request    pap⑥
        auth_accept     none⑦
        remote_name     tokyo⑧
        remote_passwd   aoshima⑨
        remote_tel      06-9999-9999⑩
```

[解　説]

・本装置Aが発信して相手（本装置B）にPPP認証で認証される場合、本装置Aのusersファイルを次のように設定します。

① 要求する認証方式（%userのauth_request）を認証なし（none）にします。
② 受け入れる認証方式（%userのauth_accept）をpapにします。
③ 認証される自局のユーザ名（%userのlocal_name）を指定します。
④ 認証される自局のパスワード（%userのlocal_passwd）を指定します。

・本装置Bが着信して相手（本装置A）をCLID認証とPPP認証で認証する場合、本装置Bのusersファイルを次のように設定します。

⑤ 着信時にCLID認証を行うように、%presetのclid_authをmustにします。
⑥ 要求する認証方式（%userのauth_request）をpapにします。
⑦ 受け入れる認証方式（%userのauth_accept）を認証なし(none）にします。
⑧ 認証する相手のユーザ名（%userのremote_name）を指定します。
⑨ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑩ CLID認証で着信を許可する相手の電話番号（%userのremote_tel）を指定します。

[参　考]

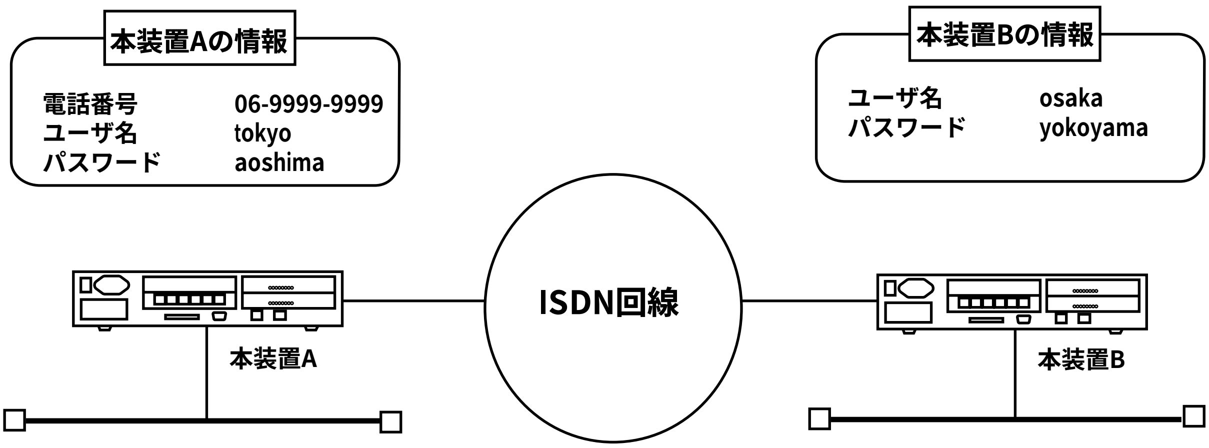
・本装置Aが発信したときは相手にPPP認証で認証され、かつ、着信したときは相手をCLID認証とPPP認証で認証する場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

```
%preset
       clid_auth            must①
%user
       auth_request         pap-②
       auth_accept          pap-③
       remote_name          osaka④
       remote_passwd        yokoyama⑤
       local_name           tokyo⑥
       local_passwd         aoshima⑦
       remote_tel           06-9999-9999⑧
```

① 着信時にCLID認証を行うように、%presetのclid_authをmustにします。
② 要求するPPP認証方式（%userのauth_request）を"着信時のみPAPを要求する"（pap-）にします。
③ 受け入れる認証方式（%userのauth_accept）を"発信時のみPAPを受け入れる"（pap-）にします。
④ 着信時に認証する相手のユーザ名（%userのremote_name）を指定します。
⑤ 着信時に認証する相手のパスワード（%userのremote_passwd）を指定します。
⑥ 発信時に認証される自局のユーザ名（%userのlocal_name）を指定します。
⑦ 発信時に認証される自局のパスワード（%userのlocal_passwd）を指定します。
⑧ CLID認証で着信を許可し、かつ発信時に電話をかけるための相手の電話番号（%userのremote_tel）を指定します。

(2) CLID認証とPPP認証（PAP）による両方向認証の併用



[本装置Aのusersファイルの設定]

```
%preset

%user
        auth_request     pap①
        auth_accept      pap②
        remote_name      osaka③
        remote_passwd    yokoyama④
        local_name       tokyo⑤
        local_passwd     aoshima⑥
```

[本装置Bのusersファイルの設定]

```
%preset
        clid_auth        must⑦
%user
        auth_request     pap⑧
        auth_accept      pap⑨
        remote_name      tokyo⑩
        remote_passwd    aoshima⑪
        local_name       osaka⑫
        local_passwd     yokoyama⑬
        remote_tel       06-9999-9999⑭
```

[解　説]

・本装置Aが発信して相手（本装置B）にPPP認証で認証され、かつ、相手をPPP認証で認証する場合、本装置Aのusersファイルを次のように設定します。
① 要求する認証方式 （%userのauth_request）をpapにします。
② 受け入れる認証方式（%userのauth_accept）をpapにします。
③ 認証する相手のユーザ名（%userのremote_name）を指定します。
④ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑤ 認証される自局のユーザ名（%userのlocal_name）を指定します。
⑥ 認証される自局のパスワード（%userのlocal_passwd）を指定します。

・本装置Bが着信して相手（本装置A）をCLID認証とPPP認証で認証し、かつ、相手にPPP認証で認証される場合、本装置Bのusersファイルを次のように設定します。
⑦ 着信時にCLID認証を行うように、%presetのclid_authをmustにします。
⑧ 要求する認証方式（%userのauth_request）をpapにします。
⑨ 受け入れる認証方式（%userのauth_accept）をpapにします。
⑩ 認証する相手のユーザ名（%userのremote_name）を指定します。
⑪ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑫ 認証される自局のユーザ名（%userのlocal_name）を指定します。
⑬ 認証される自局のパスワード（%userのlocal_passwd）を指定します。
⑭ CLID認証で着信を許可する相手の電話番号（%userのremote_tel）を指定します。

[参　考]

・本装置Aが発信したときも着信したときも、相手をPPP認証で認証し、かつ、相手にPPP認証で認証される場合で、着信したときは相手をCLID認証もする場合、本装置Aのusersファイルを次のように設定します。

[本装置Aのusersファイルの設定]

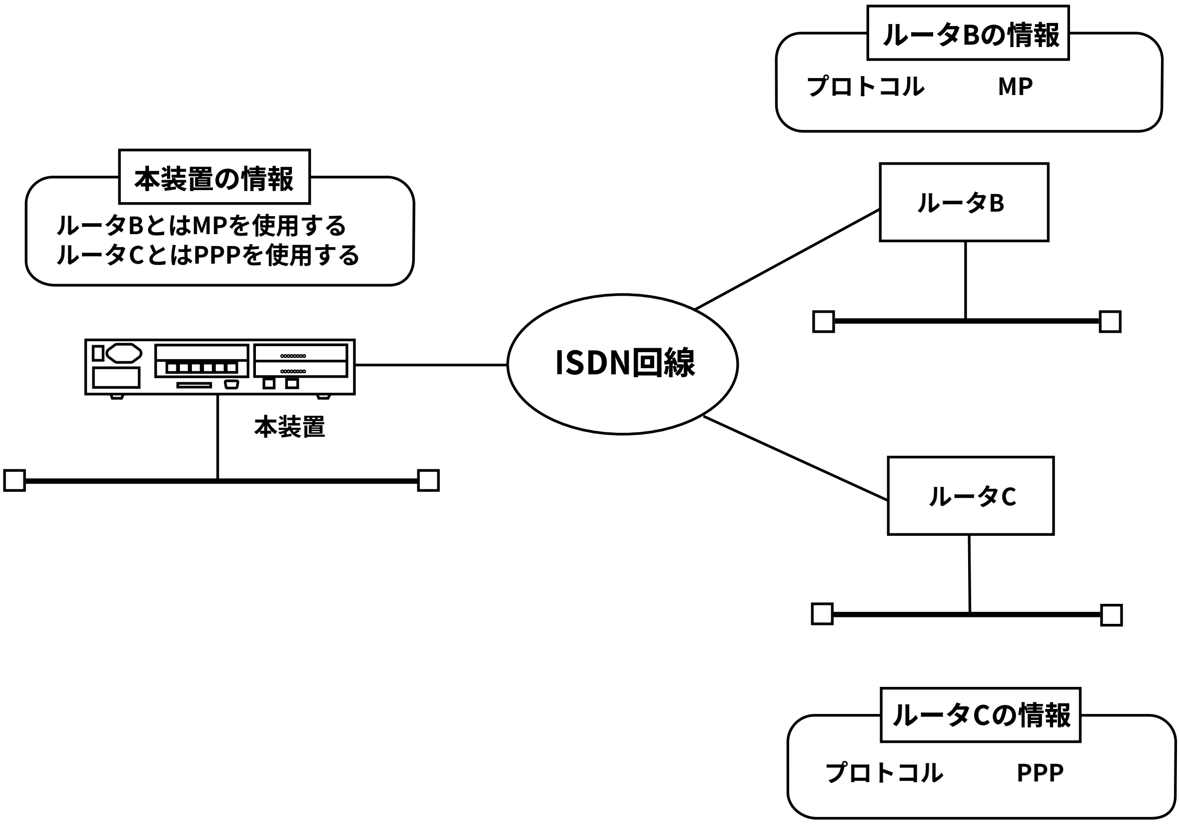
```
%preset
      clid_auth          must①
%user
      auth_request       pap②
      auth_accept        pap③
      remote_name        osaka④
      remote_passwd      yokoyama⑤
      local_name         tokyo⑥
      local_passwd       aoshima⑦
      remote_tel         06-9999-9999⑧
```

① 着信時にCLID認証を行うように、%presetのclid_authをmustにします。
② 要求するPPP認証方式 （%userのauth_request）をpapにします。
③ 受け入れる認証方式（%userのauth_accept）をpapにします。
④ 認証する相手のユーザ名（%userのremote_name）を指定します。
⑤ 認証する相手のパスワード（%userのremote_passwd）を指定します。
⑥ 認証される自局のユーザ名（%userのlocal_name）を指定します。
⑦ 認証される自局のパスワード（%userのlocal_passwd）を指定します。
⑧ CLID認証で着信を許可し、かつ発信時に電話をかけるための相手の電話番号（%userのremote_tel）を指定します。

4.4.4 MPを使用する場合の設定

ここでは、MP（Multi-Link Protocol）を使用する場合の設定方法について説明します。設定例においては、MPの設定に関連する部分のみ記述しています。

(1) MPの設定



［本装置のusersファイルの設定］

```
%preset
        protocol                mp①

%user   # ルータBに対する設定
        protocol                mp②

%user   # ルータCに対する設定
        protocol                ppp③
```

［解　説］

① 着信時に受け入れるプロトコル（%presetのprotocol）をmpにします。
この場合、接続相手からMPで要求されるとMPで接続し、PPPで要求されるとPPPで接続します。

② 本装置が発信してルータBと接続するプロトコル（%userのprotocol）をmpにします。

③ 本装置が発信してルータCと接続するプロトコル（%userのprotocol）をpppにします。

注　意　　**BACPを使用する場合は、MPを使用する場合の設定とほとんど同じで、protocolの設定のみ異なります。**
（%presetのprotocol bacpと%userのprotocol bacp）

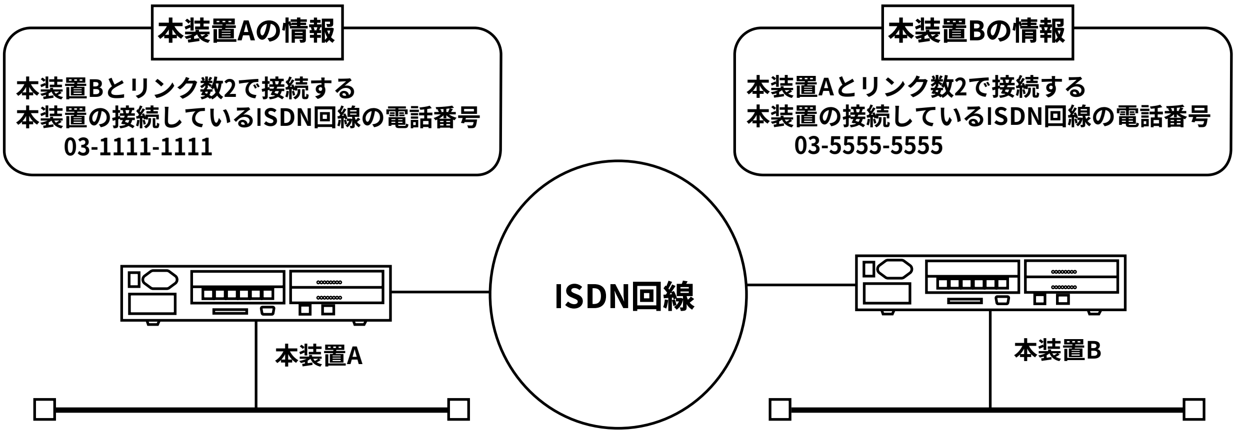
［参　考］

・MPを使用する場合には、設定例の他に**表4-1**のキーワードで動作を指定することができます。通常は変更する必要がないため、デフォルトで使用します。デフォルト値で使用する場合には、キーワードを設定する必要はありません。

表4-1　MPに関連するキーワード一覧

キーワード	機　能	設定値	デフォルト値
mp_port_min	MPで発信時に最初に接続するリンク数の設定	1～8	1
mp_port_max	MPで最大接続リンク数の設定	1～8	2
bod	MPでBOD機能を使用するかどうかの設定	on　：BOD機能を使用する off　：BOD機能を使用しない	on
bod_ctl	MPでBOD機能を動作させる条件の設定	out　：発信時のみBOD機能を使用する in　：着信時のみBOD機能を使用する both ：発信時、着信時ともにBOD機能を使用する	out
bod_add_rate	BODでリンクを増加させる転送レート(%)の設定	10～90	70
bod_del_rate	BODでリンクを減少させる転送レート(%)の設定	10～90	30
bod_sample_time	BODで転送レートを算出する平均化時間（秒）を設定	5～60	15

(2) 常時リンク数2でMP接続する場合の設定



[本装置Aのusersファイルの設定]

```
%preset
        protocol     mp①

%user
        protocol     mp②
        bod          off③
        mp_port_min  2④
        mp_port_max  2⑤
        remote_tel   03-5555-5555⑥
```

[本装置Bのusersファイルの設定]

```
%preset
        protocol     mp①

%user
        protocol     mp②
        bod          off③
        mp_port_min  2④
        mp_port_max  2⑤
        remote_tel   03-1111-1111⑥
```

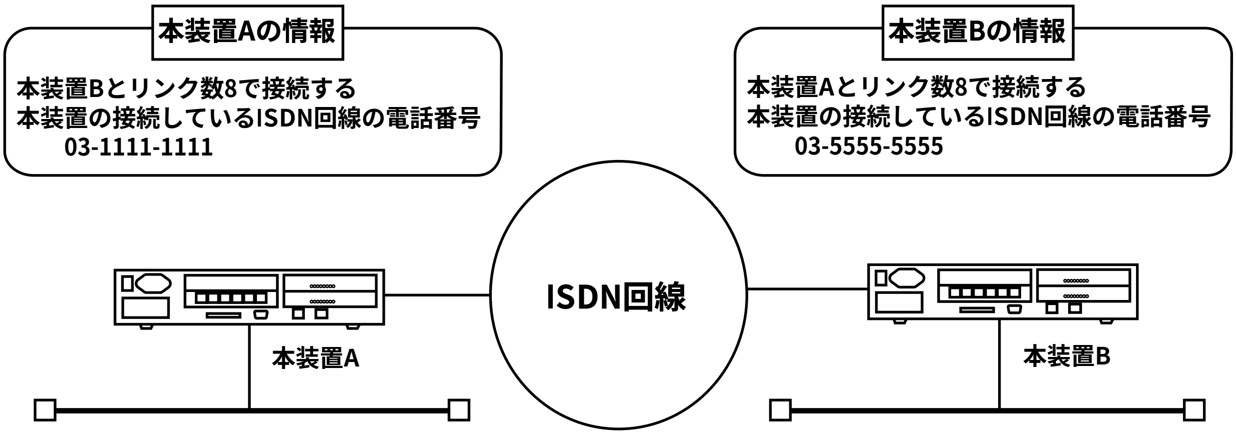
[解　説]

① 着信時に受け入れるプロトコル（%presetのprotocol）をmpにします。
② 本装置Aと本装置Bが発信する時に使用するプロトコル（%userのprotocol）をmpにします。
③ BOD機能は使用しないので、%userのbodをoffにします。
④ 本装置Aおよび本装置Bが発信して接続するリンク数（%userのmp_port_min）を2にします。
⑤ 最大接続リンク数（%userのmp_port_max）を2にします。
以上の設定により、通信開始時にリンク数が2本になり、以後、転送レートの増減によりリンク数は変化しません。
⑥ 接続する相手の電話番号（%userのremote_tel）を設定します。

注　意　　**mp_port_minを2に設定しても、通信開始時に2本目のリンクの接続に失敗した場合、本装置は2本目のリンクの再接続は行いません。このような場合、bodをonに設定すれば、その後、転送レートの増加によって2本目の再接続を行います。**

(3) MP接続でリンク数を最大8本まで使用する場合の設定

2台の本装置をMP（最大リンク数8）で接続する場合を例に説明します。



［本装置Aのusersファイルの設定］

```
%preset
        protocol     mp①

%user
        protocol     mp②
        mp_port_min  1③
        mp_port_max  8④
        remote_tel   03-5555-5555⑤
```

［本装置Bのusersファイルの設定］

```
%preset
        protocol     mp①

%user
        protocol     mp②
        mp_port_min  1③
        mp_port_max  8④
        remote_tel   03-1111-1111⑤
```

［解　説］

① 着信時に受け入れるプロトコル（%presetのprotocol）をmpにします。

② 本装置Aと本装置Bが発信する時に使用するプロトコル（%userのprotocol）をmpにします。

③ 本装置Aおよび本装置Bが発信時に、接続するリンク数（%userのmp_port_min）を1にします。

④ 最大接続リンク数（%userのmp_port_max）を8にします。
以上の設定により、通信開始時にはリンク数が1本ですが、転送レートが高くなるとBOD機能によりリンクを追加します。最大8本のリンクを使用できることになります。

⑤ 接続する相手の電話番号（%userのremote_tel）を設定します。

注　意　**本設定例では、%userにBOD機能に関する設定は行っていませんが、デフォルトで "bod on" （BOD機能を使用する）、"bod_ctl out"（発信時のみBOD機能を使用する） になっていますので、1本目のリンクが確立した時に、発信した装置側のBOD機能が有効になります。**

4.4.5　コールバック機能を使用する場合の設定

(1) 概　要

本装置は、CBCP (CallBack Control Protocol : Microsoftコールバック方式)と、独自方式の無課金コールバックをサポートしています。

・CBCP

CBCPは、Windowsが備えるコールバック方式で、接続相手から本装置に対して着信した場合、一旦ISDN回線を接続し認証を行った後、CBCPでコールバックのネゴシエーションが行われます。

その後、ISDN回線を切断し、本装置から自動的に発信（コールバック）して接続します。

本方式の場合は、一旦ISDN回線が接続されますので、相手側に最低限の料金が課金されます。

・無課金コールバック

無課金コールバックは、本装置独自の方式であり、接続相手から本装置に対して着信した場合、ISDN回線を接続する前に、発信元電話番号を利用して認証を行います（CLID認証）。

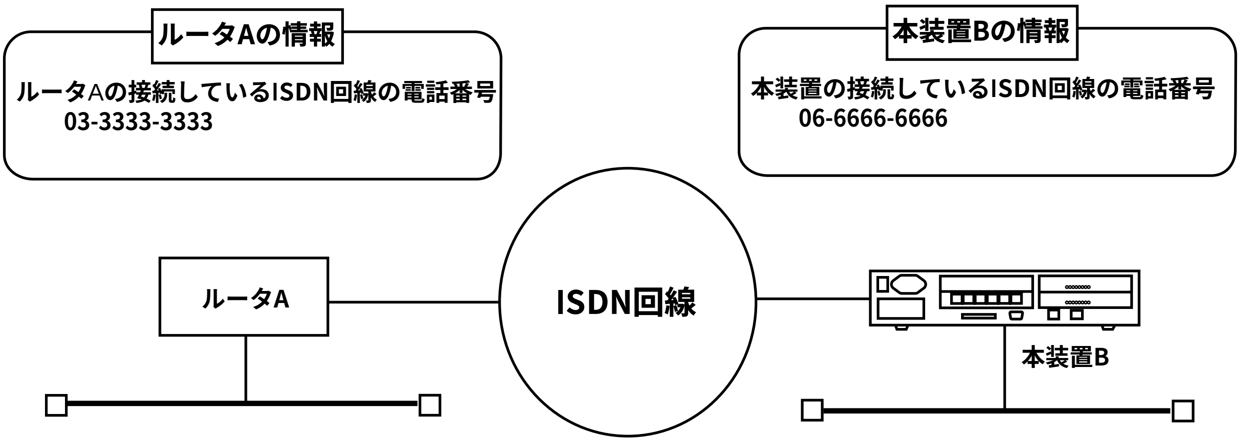
接続相手が確認できたならば、着信動作を終了し、本装置から自動的に発信（コールバック）して接続します。

本方式の場合は、ISDN回線は接続してませんので、相手側に料金が課金されることはありません。

注　意　　**無課金コールバックは、本装置独自方式であるため、本装置以外と接続した場合の動作は、保証しません。**

(2) CBCPのコールバック要求を受け入れる場合の設定

ここでは、本装置BがルータAからのCBCPのコールバック要求を受け入れる場合の設定方法について説明します。
設定例においては、CBCPのコールバックの設定に関連する部分のみ記述しています。



[本装置Bのusersファイルの設定]

```
%user   # ルータAに対する設定
        cb              accept①
        cb_type         cbcp②
        cb_mode         may③

        remote_tel      03-3333-3333④
```

[解　説]

・本装置BがルータAからのCBCPのコールバック要求を受け入れ、相手（ルータA）へコールバックする場合、本装置Bのusersファイルを次のように設定します。

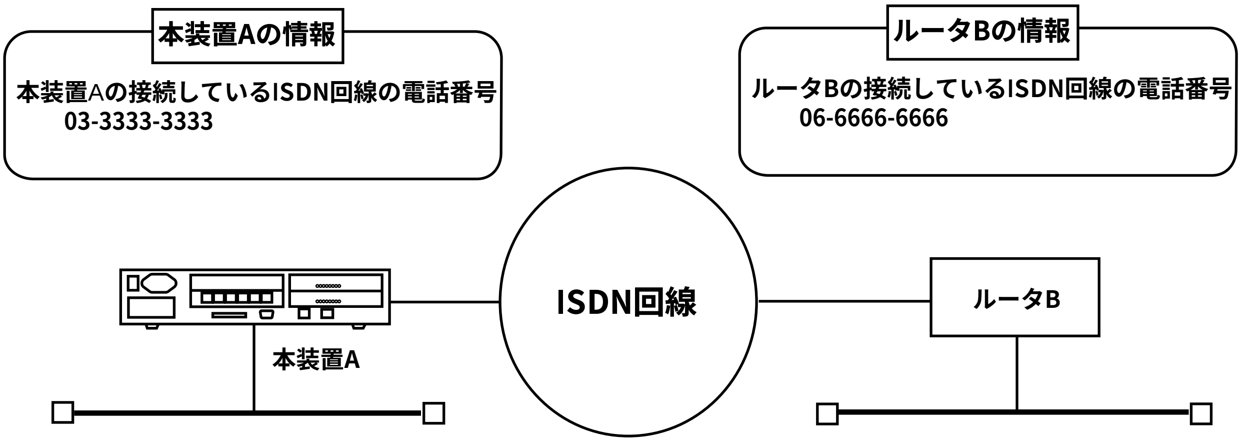
① ルータAからのコールバック要求を受け入れる設定にします（%userのcb accept）。
② 受け入れるコールバック方式（%userのcb_type）をcbcpにします。
③ 受け入れるコールバックの動作モード（%userのcb_mode）をmayにします。
mayを設定した場合は、ルータAがコールバック要求を発行してこなかった時、通常の着信動作で接続します。
（mustを設定した場合は、ルータAがコールバック要求を発行してこなかった時、着信を拒否し、接続しません）

本装置Bは、ルータAからのコールバック要求を受け入れて、呼が切断されたならば、%userのremote_telキーワード（④）で設定された相手電話番号にコールバックします。

[参　考] (6) コールバック機能使用時の注意事項

(3) CBCPのコールバック要求を発行する場合の設定

ここでは、本装置AからルータBに対してCBCPのコールバック要求を発行する場合の設定方法について説明します。
設定例においては、CBCPのコールバックの設定に関する部分のみ記述しています。



［本装置Aのusersファイルの設定］

```
%user   # ルータBに対する設定
        cb              request①
        cb_type         cbcp②
        cb_mode         may③

        remote_tel      06-6666-6666④
```

［解　説］

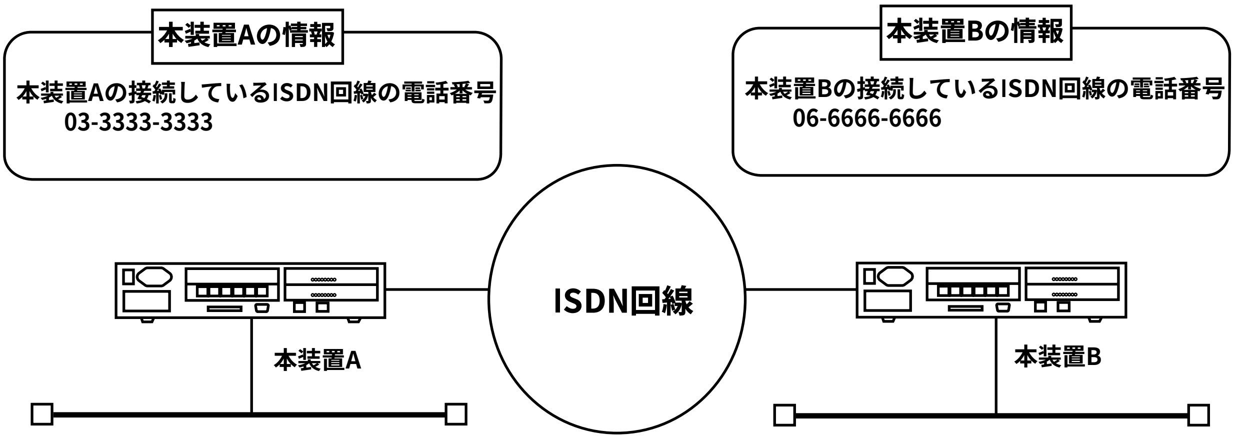
・本装置AからルータBに対してCBCPのコールバック要求を発行して、相手（ルータB)からコールバックされる場合、本装置Aのusersファイルを次のように設定します。

① ルータBへ発信時、コールバック要求を発行する設定をします（%userのcb request）。
② 要求するコールバック方式（%userのcb_type）をcbcpにします。
③ 要求するコールバックの動作モード（%userのcb_mode）をmayにします。
mayを設定した場合は、ルータBがコールバック要求を受け入れなかった時、通常の着信動作で接続します。
（mustを設定した場合は、ルータBがコールバック要求を受け入れなかった時、発信失敗となり接続しません）
④ 発信する相手電話番号を設定します。

［参　考］ **(6) コールバック機能使用時の注意事項**

(4) 無課金コールバックを使用する設定

ここでは、本装置Aから本装置Bに対して無課金コールバック要求を発行する場合の設定方法について説明します。
設定例においては、無課金コールバックの設定に関する部分のみ記述しています。



[本装置Aのusersファイルの設定]

```
%user   # 本装置Bに対する設定
        cb            request①
        cb_type       isdn②



        remote_tel    06-6666-6666③
```

[本装置Bのusersファイルの設定]

```
%preset
      clid_auth     must④

%user   # 本装置Aに対する設定
        cb            accept⑤
        cb_type       isdn⑥

        remote_tel    03-3333-3333⑦
```

[解　説]

・本装置Aから本装置Bに対して無課金コールバック要求を発行して、相手（本装置B)からコールバックされる場合、本装置Aのusersファイルを次のように設定します。

① 本装置Bへ発信時、コールバック要求を発行する設定をします（%userのcb request）。
② 要求するコールバック方式（%userのcb_type）をisdnにします。
③ 発信する相手電話番号を設定します。

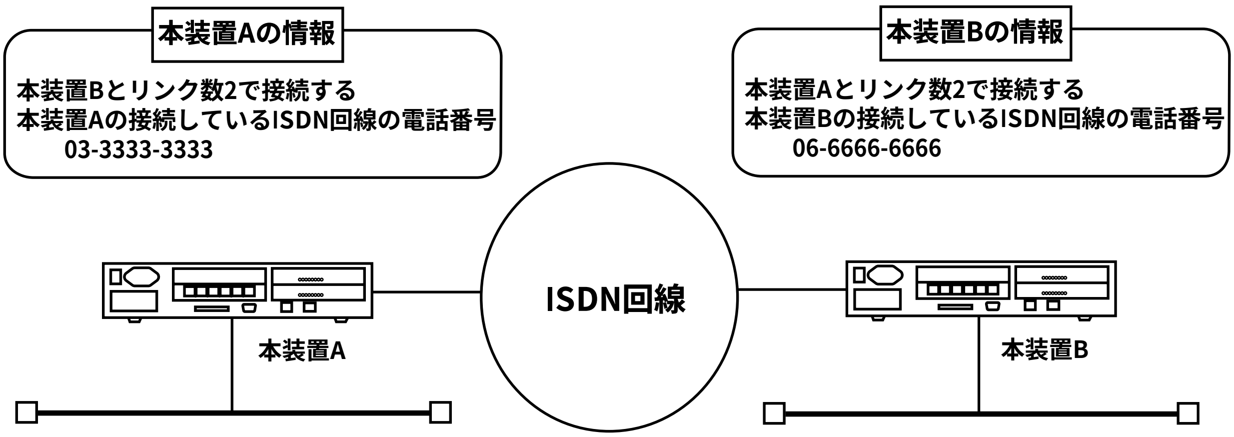
・本装置Bが本装置Aからの無課金コールバック要求を受け入れ、相手（本装置A）へコールバックする場合、本装置Bのusersファイルを次のように設定します。

④ 着信時にCLID認証を行うように、%presetのclid_authをmustにします。
（mayを設定し、CLID認証が失敗した場合は、通常の着信動作で接続します）
⑤ 本装置Aから着信時、コールバック要求を受け入れる設定をします (%userのcb accept)。
⑥ 受け入れるコールバック方式（%userのcb_type）をisdnにします。
⑦ CLID認証で着信を許可する相手の電話番号（%userのremote_tel）を設定します。

本装置Bは、本装置Aからのコールバック要求を受け入れて、着信動作終了後、%userのremote_telキーワード（⑦）で設定された相手電話番号にコールバックします。

(5) MPでCBCPのコールバックを使用する設定

ここでは、本装置Aから本装置Bに対してMPでCBCPのコールバック要求を発行する場合の設定方法について説明します。
設定例においては、MPとCBCPコールバックの設定に関する部分のみ記述しています。



[本装置Aのusersファイルの設定]

```
%preset
        protocol      mp①

%user   # 本装置Bに対する設定
        protocol      mp②
        bod           off③

        mp_port_max   2④
        cb            request⑤
        cb_type       cbcp⑥
        cb_mode       may⑦

        remote_tel    06-6666-6666⑧
```

[本装置Bのusersファイルの設定]

```
%preset
        protocol      mp⑨

%user   # 本装置Aに対する設定
        protocol      mp⑩
        bod           off⑪
        mp_port_min   2⑫
        mp_port_max   2⑬
        cb            accept⑭
        cb_type       cbcp⑮
        cb_mode       may⑯

        remote_tel    03-3333-3333⑰
```

[解　説]

・本装置Aから本装置Bに対してCBCPのコールバック要求を発行して、相手（本装置B)からコールバックされる場合、本装置Aのusersファイルを次のように設定します。

① 本装置Bからコールバックされた時（着信時）に、受け入れるプロトコル（%presetのprotocol）をmpにします。
② 本装置Aが発信して、相手と接続するプロトコル（%userのprotocol）をmpにします。
③ BOD機能は使用しないので、%userのbodをoffにします。
④ mpの最大接続リンク数（%userのmp_port_max）を2にします。

⑤ 本装置Bへ発信時、コールバック要求を発行する設定をします（%userのcb request）。
⑥ 要求するコールバック方式（%userのcb_type）をcbcpにします。
⑦ 要求するコールバックの動作モード（%userのcb_mode）をmayにします。
mayを設定した場合は、本装置Bがコールバック要求を受け入れなかった時、通常の発信動作で接続します。
（mustを設定した場合は、本装置Bがコールバック要求を受け入れなかった時、発信失敗となり接続しません）
⑧ 発信する相手電話番号を設定します。

・本装置Bが本装置AからのCBCPのコールバック要求を受け入れ、相手（本装置A）へコールバックする場合、本装置Bのusersファイルを次のように設定します。

⑨ 着信時に受け入れるプロトコル（%presetのprotocol）をmpにします。
⑩ 本装置Aと接続するプロトコル（%userのprotocol）をmpにします。
⑪ BOD機能は使用しないので、%userのbodをoffにします。
⑫ %userのmp_port_minキーワードは、コールバックを受け入れた場合、コールバックで接続するリンク数になります。接続するリンク数を2にします。
⑬ MPの最大接続リンク数（%userのmp_port_max）を2にします。

⑭ 本装置Aから着信時、コールバック要求を受け入れる設定をします（%userのcb accept）。
⑮ 受け入れるコールバック方式（%userのcb_type）をcbcpにします。
⑯ 受け入れるコールバックの動作モード（%userのcb_mode）をmayにします。
mayを設定した場合は、本装置Aがコールバック要求を発行してこなかった時、通常の着信動作で接続します。
（mustを設定した場合は、本装置Aがコールバック要求を発行してこなかった時、着信を拒否し、接続しません）

本装置Bは、本装置Aからのコールバック要求を受け入れて、呼が切断されたならば、%userのremote_telキーワード（⑰）で設定された相手電話番号に対して、%userのmp_port_minキーワード（⑫）で設定されたリンク数分、コールバックします。

注　意　**BACPでCBCPのコールバックを使用する場合は、MPでCBCPのコールバックを使用する場合の設定とほとんど同じでprotocolの設定のみ異なります。（%presetのprotocol bacpと%userのprotocol bacp）**

［参　考］(6) コールバック機能使用時の注意事項

4章　各種機能の設定方法

(6) コールバック機能使用時の注意事項

●本装置がコールバック要求を受け入れてコールバックする場合、次のどちらかの相手電話番号に対して行います。

・%userのremote_telキーワードで設定された相手電話番号。

・着信時に、発信元電話番号通知で通知された相手電話番号。

両方とも有効な場合は、設定された相手電話番号（%userのremote_telキーワード）が優先されます。
両方とも無効な場合は、接続相手に対して、CBCPのプロトコルを使用してコールバックする電話番号の問い合わせを行い、相手から通知された電話番号にコールバックします。

●本装置がコールバック要求を発行し、相手からCBCPのプロトコルを使用してコールバックする電話番号の問い合わせを受け付けた場合は、本装置の発呼で使用したboardsファイルのtelnumberキーワードで設定された自局電話番号を通知します。
もし、telnumberキーワードで自局電話番号が設定されていない場合は、コールバック失敗となり、接続できません。

●本装置とMP対応のTA（ターミナルアダプタ）とコールバック接続する場合の注意
Windowsマシン+TAから本装置に対してコールバック要求を発行しても、TAの仕様により、このコールバック要求が本装置に通知されないことがあり、コールバックできない場合があります。
この現象は、TAがMPで動作する場合だけであり、PPPの場合は問題ありません。

●RADIUS認証サーバを使用した無課金コールバックはできません。

4.4.6 回線自動切断の設定

ここでは、回線を自動切断する場合の設定方法について説明します。本装置は、アイドル監視による回線自動切断機能と、連続接続時間による回線自動切断機能をサポートしています。設定例には、回線自動切断の設定部分のみについて記述しています。

(1) アイドル監視による回線自動切断について

設定された時間、アイドル状態(データが流れていない状態)を検出すると、ISDN回線を切断します。
アイドル監視による回線自動切断は、**表4-2**のusersファイルのキーワードで動作を指定することができます。

表4-2　アイドル監視による回線自動切断に関連するusersファイルのキーワード一覧

キーワード	機　能	設　定　値	デフォルト値
auto_disconnect	アイドル監視による回線自動切断を行うかどうかの設定	on　：行う off　：行わない	on
idle_timeout	タイムアウト時間の設定（秒単位）	5～100000	120
idle_ctl	発着信のいずれの場合にアイドル監視を行うかの設定	both ：発信も着信も行う in　：着信のみ行う out　：発信のみ行う	both
idle_timeout_in	着信時のタイムアウト時間の設定（秒単位）	5～100000	なし
idle_timeout_out	発信時のタイムアウト時間の設定（秒単位）	5～100000	なし

(2) 連続接続時間による回線自動切断について

連続接続時間が設定された時間を超えた場合に、ISDN回線を切断します。
連続接続時間による回線自動切断は、**表4-3**のusersファイルのキーワードで動作を指定することができます。

表4-3　連続接続時間による回線自動切断に関連するusersファイルのキーワード一覧

キーワード	機　能	設　定　値	デフォルト値
session_disconnect	連続接続時間による回線自動切断行うかどうかの設定	on :行う off:行わない	off
session_timeout	タイムアウト時間の設定(秒単位)	5～100000	3600

(3) RADIUS認証サーバでの設定

RADIUS認証サーバに設定する場合は、Idle-Timeout アトリビュート、Session-Timeout アトリビュートを使用します。

- RADIUS認証サーバでIdle-Timeout アトリビュートの値を設定すると、この値をidle_timeout キーワードの値と解釈し、かつauto_disconnect キーワードを「on」と解釈します。ただし、Idle-Timeout アトリビュートの値が0に設定された場合は、auto_disconnect キーワードが「off」と解釈され、アイドル監視による自動切断機能はoffになります。

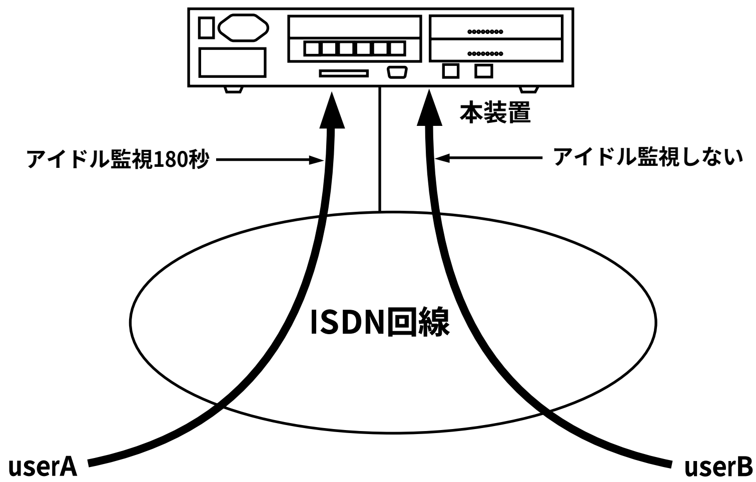
- RADIUS認証サーバでSession-Timeout アトリビュートの値を設定すると、この値をsession_timeout キーワードの値と解釈し、かつsession_disconnect キーワードを「on」と解釈します。ただし、Session-Timeout アトリビュートの値が0に設定された場合は、session_disconnect キーワードが「off」と解釈され、連続接続時間による回線自動切断機能はoffになります。

(4) アイドル監視による回線自動切断の設定

ここでは、

- userAに対しては、アイドル監視時間180秒の回線自動切断を行う。
- userBに対しては、アイドル監視による回線自動切断を行わない。

という場合の設定例について説明します。



[本装置のusersファイルの設定]

```
# userAに対する設定
%user
    auto_disconnect         on①
    idle_timeout            180②

# userBに対する設定
%user
    auto_disconnect         off③
```

[解　説]

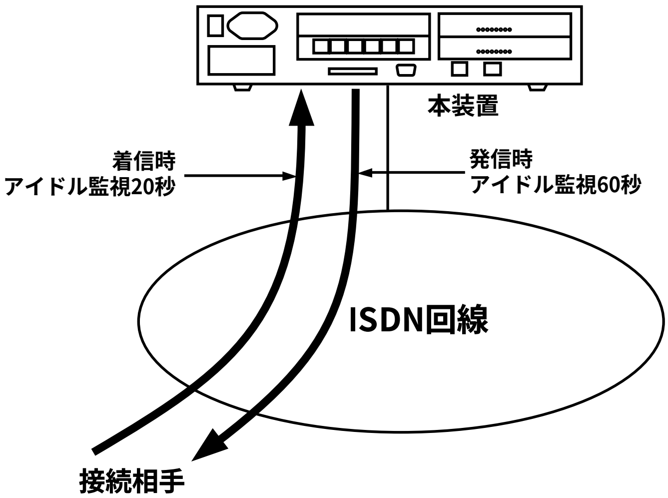
① userAに対する設定で、アイドル監視による回線自動切断(auto_disconnect)を行う設定(on)にします。
② userAに対する設定で、アイドル監視時間(idle_timeout)を180秒に設定します。
③ userBに対する設定で、アイドル監視による回線自動切断(auto_disconnect)を行わない設定(off)にします。

(5) 発信か着信かでアイドル監視時間を変える設定

ここでは、

- 本装置が発信側の場合には、アイドル監視時間60秒の回線自動切断を行う。
- 本装置が着信側の場合には、アイドル監視時間20秒の回線自動切断を行う。

という場合の設定例について説明します。



[本装置のusersファイルの設定]

```
%user
    auto_disconnect         on①
    idle_timeout_out        60②
    idle_timeout_in         20③
```

[解　説]

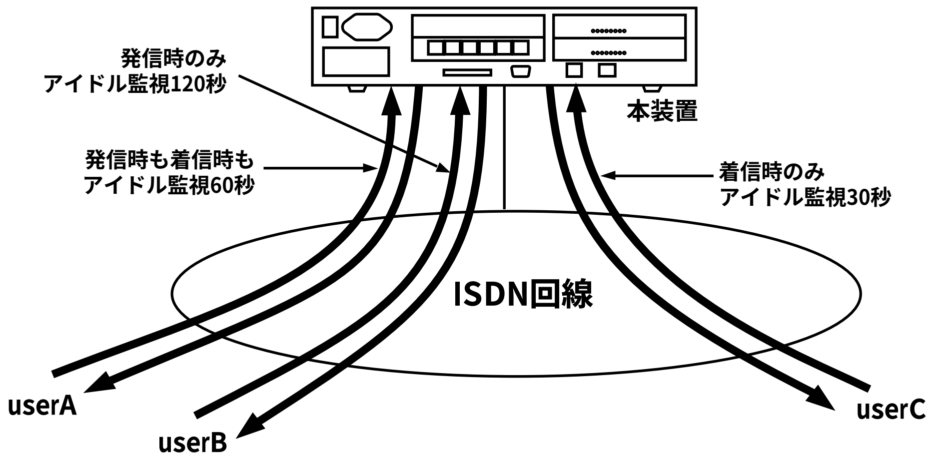
① アイドル監視による回線自動切断(auto_disconnect)を行う設定(on)にします。
② 発信時のアイドル監視時間(idle_timeout_out)を60秒に指定します。
③ 着信時のアイドル監視時間(idle_timeout_in)を20秒に指定します。

(6) 発信時のみまたは着信時のみアイドル監視を行う設定

ここでは、

- userAに対しては、発信時も着信時もアイドル監視時間60秒の回線自動切断を行う。
- userBに対しては、発信時のみアイドル監視時間120秒の回線自動切断を行い、着信時はアイドル監視による回線自動切断を行わない。
- userCに対しては、着信時のみアイドル監視時間30秒の回線自動切断を行い、発信時はアイドル監視による回線自動切断を行わない。

という場合の設定例について説明します。



［本装置のusersファイルの設定］

```
# userAに対する設定
%user
    auto_disconnect                 on①
    idle_timeout                    60②
    idle_ctl                        both③

# userBに対する設定
%user
    auto_disconnect                 on④
    idle_timeout                    120⑤
    idle_ctl                        out⑥

# userCに対する設定
%user
    auto_disconnect                 on⑦
    idle_timeout                    30⑧
    idle_ctl                        in⑨
```

[解　説]

① userAに対する設定で、アイドル監視による回線自動切断(auto_disconnect)を行う設定(on)にします。

② userAに対する設定で、アイドル監視時間(idle_timeout)を60秒に指定します。

③ userAに対する設定で、発信時も着信時もアイドル監視を行うことを指定します(idle_ctlをbothに指定します)。

④ userBに対する設定で、アイドル監視による回線自動切断(auto_disconnect)を行う設定(on)にします。

⑤ userBに対する設定で、アイドル監視時間(idle_timeout)を120秒に指定します。

⑥ userBに対する設定で、発信時のみアイドル監視を行うことを指定します(idle_ctlをoutに指定します)。

⑦ userCに対する設定で、アイドル監視による回線自動切断(auto_disconnect)を行う設定(on)にします。

⑧ userCに対する設定で、アイドル監視時間(idle_timeout)を30秒に指定します。

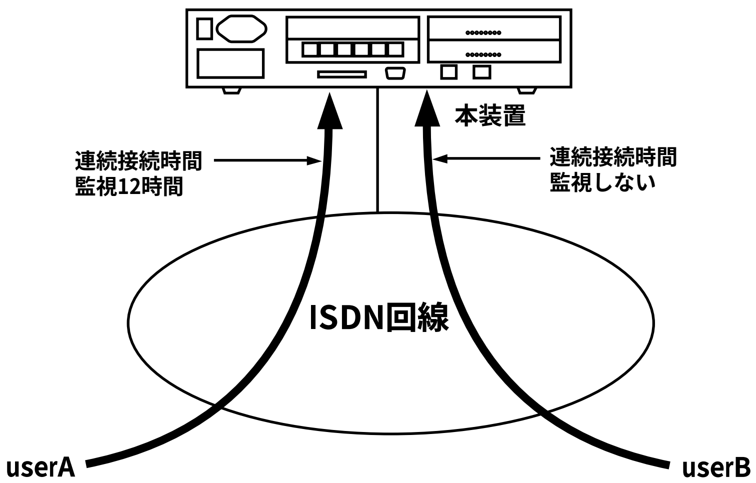
⑨ userCに対する設定で、着信時のみアイドル監視を行うことを指定します(idle_ctlをinに指定します)。

(7) 連続接続時間による回線自動切断の設定

ここでは、

- userAに対しては、連続接続時間が12時間に達した場合に自動切断する。
- userBに対しては、連続接続時間による自動切断を行わない。

という場合の設定例について説明します。



[本装置のusersファイルの設定]

```
# userAに対する設定
%user
    session_disconnect      on①
    session_timeout         43200②

# userBに対する設定
%user
    session_disconnect      off③
```

[解　説]

① userAに対する設定で、連続接続時間による回線自動切断(session_disconnect)を行う設定(on)にします。

② userAに対する設定で、連続接続監視時間(session_timeout)を43200秒(12時間)に指定します。

③ userBに対する設定で、連続接続時間による回線自動切断(session_disconnect)を行わない設定(off)にします。

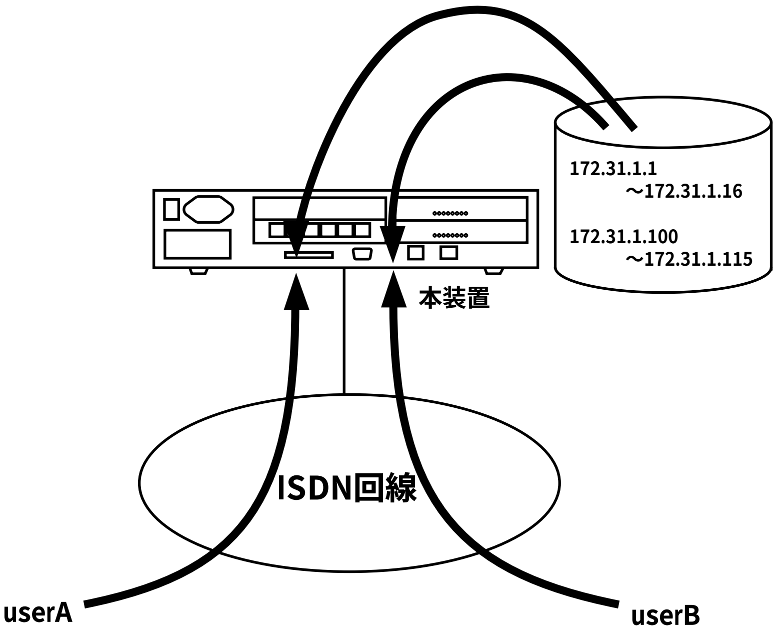
4章 各種機能の設定方法

4.4.7 IPプールを使用する場合の設定

ここでは、IPプールを使って接続相手にIPアドレスを割り当てる場合の設定方法について説明します。設定例には、IPアドレス割り当ての設定部分のみについて記述しています。

(1) １つのIPプールのみを使用する場合の設定

ここでは、IPプールに、
172.31.1.1〜172.31.1.16
172.31.1.100〜172.31.1.115
の合計32個のIPアドレスをプールし、このプールから接続相手にIPアドレスを割り当てる場合の設定例について説明します。



［本装置のippoolファイルの設定］

```
172.31.1.1/24        16
172.31.1.100/24      16
```

［本装置のusersファイルの設定］

```
# userAに対する設定
%user
 interface isdn0 * * unnumbered
             ppp address on * 255.255.255.254

# userBに対する設定
%user
 interface isdn0 * * unnumbered
             ppp address on * 255.255.255.254
```

(2) 複数のIPプールを使用する場合の設定

本装置では、複数のIPプールを使用して、ユーザ毎に使用するIPプールを指定することができます。

ここでは、IPプールの1番に、

172.31.1.1～172.31.1.16

172.31.1.100～172.31.1.115

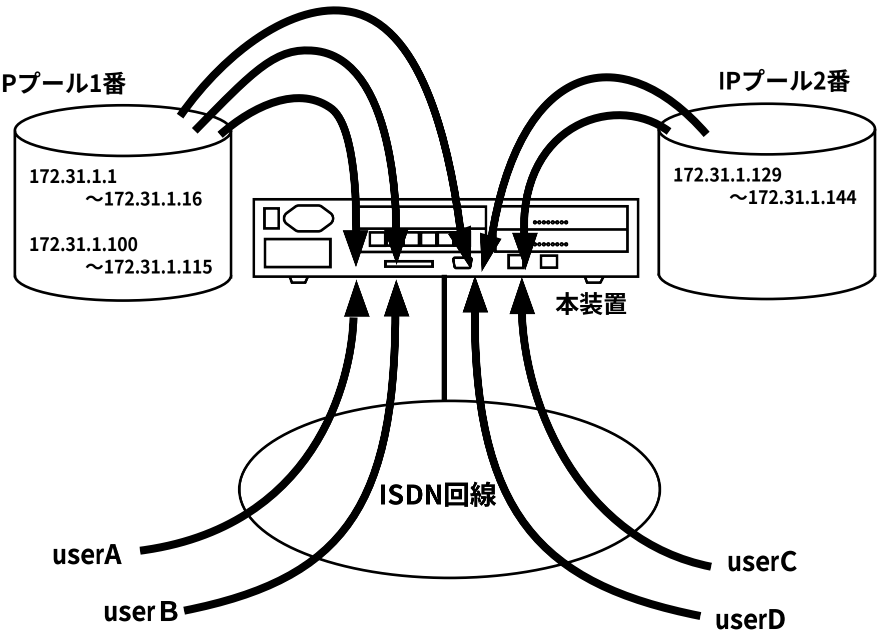
の合計32個のIPアドレスをプールし、IPプールの2番に、

172.31.1.129～172.31.1.144

の合計16個のIPアドレスをプールし、

- userA、userBに対しては、1番のプールからIPアドレスを割り当てる。
- userCに対しては、2番のプールからIPアドレスを割り当てる。
- userDに対しては、すべてのプール（ここでは1番と2番のプール）からIPアドレスを割り当てる。

という場合の設定例について説明します。



［本装置のippoolファイルの設定］

```
%ippool       1①
  172.31.1.1/24              16
  172.31.1.100/24            16
%ippool       2②
  172.31.1.129/24            16
```

［本装置のusersファイルの設定］

```
# userAに対する設定
%user
  ippool                     1③
  interface isdn0 * * unnumbered
              ppp address on * 255.255.255.254

# userBに対する設定
%user
  ippool                     1④
  interface isdn0 * * unnumbered
              ppp address on * 255.255.255.254

# userCに対する設定
%user
  ippool                     2⑤
  interface isdn0 * * unnumbered
              ppp address on * 255.255.255.254

# userDに対する設定
%user
  ippool                     0⑥
  interface isdn0 * * unnumbered
              ppp address on * 255.255.255.254
```

［解　説］

① userA、userBに割り当てるIPアドレスを、1番のプールとしてippoolファイルに登録します。

② userCに割り当てるIPアドレスを、2番のプールとしてippoolファイルに登録します。

③ usersファイルのuserAに対する設定で、1番のプールからIPアドレスを割り当てるように設定します。

④ usersファイルのuserBに対する設定で、1番のプールからIPアドレスを割り当てるように設定します。

⑤ usersファイルのuserCに対する設定で、2番のプールからIPアドレスを割り当てるように設定します。

⑥ usersファイルのuserDに対する設定で、ippoolファイルに設定されているすべてのプールから空いているIPアドレスを検索し、見つかったIPアドレスを割り当てるように設定します。

（ここは空白のページです。）

4.5　LANポートの設定

本装置には、イーサネットに接続するためのポートとして、LAN1ポート、LAN2ポートの2つのLANポートがあります。
本装置の各LANポートは、装置内部の論理インタフェースに以下のように対応します。

LAN1ポート：論理インタフェースen0
LAN2ポート：論理インタフェースen1

本装置のLANポートを使用可能にするためには、interfaceファイルに各LANポートに対応する論理インタフェースのIPアドレス、および接続されるネットワークに関する設定を行う必要があります。interfaceファイルの詳細な設定方法については、**「5.4　interfaceファイル」**を参照してください。

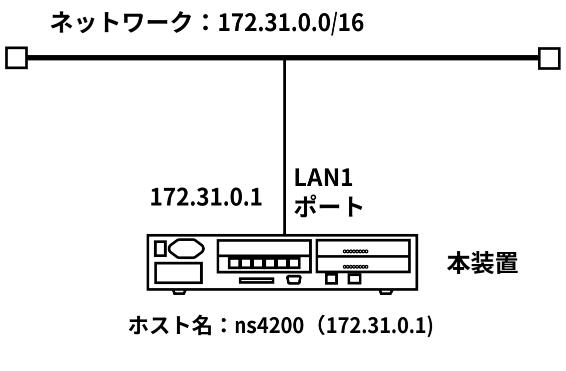
ここでは、**4.5.1**、**4.5.2**で本装置のLAN1、LAN2ポートの基本的な設定方法について説明します。さらに**4.5.3**、**4.5.4**で応用例について説明します。

4.5.1　LAN1ポートのみを使用する場合の設定

ここでは、

- LAN1ポートをネットワークアドレス172.31.0.0/16のネットワークに接続する。
- LAN1ポートの自局IPアドレスとして172.31.0.1を使用する。
- LAN2ポートを使用しない。

という場合の設定例について説明します。



この設定例のように、本装置のホスト名に対応するIPアドレスをLANポートに割り合てる場合、2種類の設定方法があります。

＜設定方法1＞

［本装置のhostnameファイルの設定］

```
ns4200①
```

［本装置のhostsファイルの設定］

```
172.31.0.1   ns4200②
```

［本装置のinterfaceファイルの設定］

```
interface   en0③   */*④   numbered
```

＜設定方法2＞

［本装置のhostnameファイルの設定］

```
ns4200①
```

［本装置のhostsファイルの設定］

```
172.31.0.1     ns4200②
```

［本装置のinterfaceファイルの設定］

```
interface  en0/172.31.0.1⑤    172.31.0.0/16⑥     numbered
```

［解　説］

① 本装置のホスト名を設定します（設定方法1、2とも同様です）。
② 本装置のホスト名に対応するIPアドレスを設定します（設定方法1、2とも同様です）。

③,④ 設定方法１の場合のinterfaceファイルの設定
論理インタフェースen0の設定を行います。設定方法１のように、論理インタフェースen0の自局IPアドレスを省略すると（③の部分）、本装置のホスト名（ns4200）に対応するIPアドレス（172.31.0.1）が割り当てられます。
また相手IPアドレスを*/*を設定することによって（④の部分）、本装置のホスト名に対応するIPアドレスのネットワークアドレス（172.31.0.0/16）が設定されます。

⑤,⑥ 設定方法２の場合のinterfaceファイルの設定
論理インタフェースen0（LAN1ポート）に172.31.0.1を自局IPアドレスとして割り当てます（⑤の部分）。
直接接続されるネットワークのアドレス（172.31.0.0）をマスク16で設定します（⑥の部分）

注　意　　LANポートが直接接続されるネットワークがサブネットである場合には、設定方法2の書式で記述します。たとえば構成図のネットワークが、172.31.0.0/24の場合には、interfaceファイルの設定は、次のように⑦の部分のマスクを24で設定します。

サブネットを使用する場合のinterfaceファイルの設定

```
interface   en0/172.31.0.1   172.31.0.0/24⑦   numbered
```

サブネットの設定に関しては、「4.6.2　サブネットマスクを使用する場合の設定」も参照してください。

注　意　　設定方法1のようなinterfaceファイルの設定方法で、本装置のホスト名に対応するIPアドレス、ネットワークアドレスを設定できるのは、1つの論理インタフェースのみです。したがって、en0（LAN1ポート）、en1（LAN2ポート）に同時にこのような設定をすることはできません（4.5.2参照）。

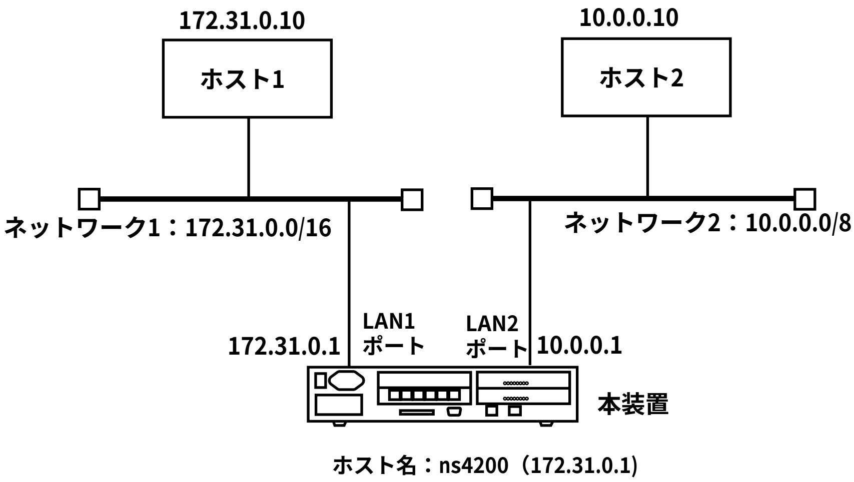
（ここは空白のページです。）

4.5.2　LAN1ポートとLAN2ポートを使用する場合の設定

ここでは、

- LAN1ポートをネットワーク1(ネットワークアドレス172.31.0.0/16)に接続する。
- LAN1ポートの自局IPアドレスとして172.31.0.1を使用する。
- LAN2ポートをネットワーク2(ネットワークアドレス10.0.0.0/8)に接続する。
- LAN2ポートの自局IPアドレスとして10.0.0.1を使用する。

という場合の設定例について説明します。



[本装置のhostnameファイルの設定]

```
ns4200①
```

[本装置のhostsファイルの設定]

```
172.31.0.1   ns4200②
```

[本装置のinterfaceファイルの設定]

```
interface   en0            */*          numbered③
interface   en1/10.0.0.1   10.0.0.0/8   numbered④
```

[解　説]

① 本装置のホスト名を設定します。

② 本装置のホスト名とIPアドレスの対応関係を設定します。

③ 論理インタフェースen0(LAN1ポートに対応)を設定します。この例の場合、自局IPアドレスとして本装置のホスト名のIPアドレス(172.31.0.1)が、相手IPアドレス/マスクとして172.31.0.0/16が設定されたことになります。以下のように設定しても同じ結果になります。

```
interface   en0/172.31.0.1   172.31.0.0/16   numbered
```

④ 論理インタフェースen1(LAN2ポートに対応)を設定します。この例の場合、自局IPアドレスとして10.0.0.1を、相手IPアドレス/マスクとして10.0.0.0/8を設定しています。

以上の設定をすることによって、LAN1ポート、LAN2ポートが使用可能になります。
またLAN1／LAN2ポート間のルーティングも可能になります。したがって、ホスト1上でネットワーク2に対するルーティング情報が設定され、ホスト2上でネットワーク1に対するルーティング情報が設定されている場合には、ホスト1、ホスト2間のIP通信も可能になります。

逆にネットワーク1、ネットワーク2間のルーティングを行いたくない場合には、以下の設定例のように論理インタフェースen0、en1にアウトプットフィルタを設定します。

[interfaceファイルの設定]

```
interface  en0/172.31.0.1    172.31.0.0/16     numbered
           outputfil    filter0
interface  en1/10.0.0.1       10.0.0.0/8       numbered
           outputfil    filter1
```

[ipfiltersファイルの設定]

```
%FILTER       filter0
            INTERFACE  !=  en1
%FILTER       filter1
            INTERFACE  !=  en0
```

このように設定することによって、たとえば論理インタフェースen0では、論理インタフェースen1以外のフレームが出力され、逆に論理インタフェースen1では、論理インタフェースen0以外のフレームが出力されることから、LAN1／LAN2ポート間のフレームがルーティングされなくなります（フィルタの設定方法については、**「4.6.1　IPフィルタ機能を使用する場合の設定」**、**「5.6　ipfiltersファイル」**を参照してください）。

注　意　**本装置上でpingコマンド、telnetコマンドを使用する場合、本装置のホスト名に対応するIPアドレスがソースアドレスとして使用されます。**
本設定例では、LAN1ポート（論理インタフェースen0）に本装置のホスト名に対応するIPアドレスが割り当てられています。したがって、ホスト１に対しては、「ping 172.31.0.10」のようにpingコマンドを実行できます。
しかし、LAN2ポート（論理インタフェースen1）には、本装置のホスト名とは異なるIPアドレスが割り当てられています。このような場合には、pingコマンド、telnetコマンドともに、-s オプションを使用してソースアドレスを指定します。たとえば、ホスト2にpingコマンドを実行する場合、

```
ping  –s 10.0.0.1  10.0.0.10
```

のように本装置のソースアドレスを指定して実行します。

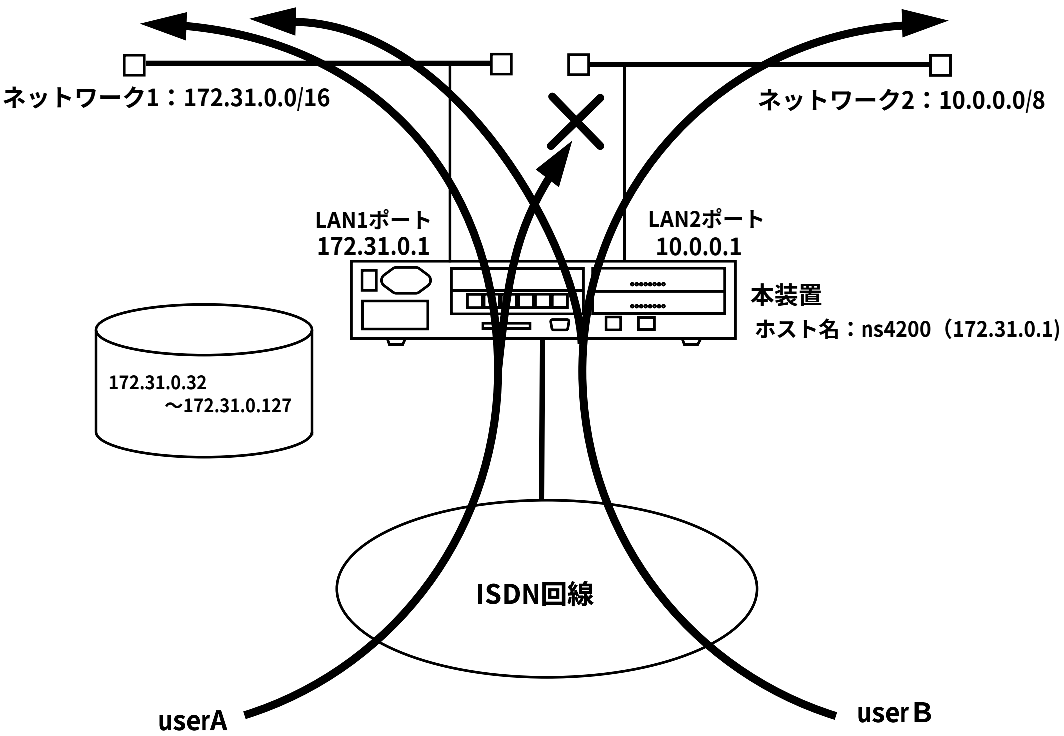
4.5.3　LAN1ポートとLAN2ポートを使用する場合の設定(端末型接続を行う場合1)

ここでは、本装置の2つのLANポートを使用し、ISDN経由で端末型接続してきた相手のユーザ名に応じてアクセスできるLANポートを限定する場合について説明します。

以下に示す例では、接続相手毎に入力パケットの制限(アクセスリスト)を分ける手法を用います。

次のようなネットワーク構成を例に説明します。

・ LAN1ポートをネットワーク1(ネットワークアドレス172.31.0.0/16)に接続する。
・ LAN1ポートの自局IPアドレスとして172.31.0.1を使用する。
・ LAN2ポートをネットワーク2(ネットワークアドレス10.0.0.0/8)に接続する。
・ LAN2ポートの自局IPアドレスとして10.0.0.1を使用する。
・ userA、userBからの端末型接続を受け付ける。ただし、userAについては、ネットワーク1へのアクセスのみを許可し、ネットワーク2へのアクセスは認めない。
・ userA、userBに対して割り当てるIPアドレスとして、172.31.0.32～172.31.0.127までの96個のIPアドレスをプールしておく。



[本装置のhostnameファイルの設定]

```
ns4200①
```

[本装置のhostsファイルの設定]

```
172.31.0.1   ns4200②
```

[本装置のinterfaceファイルの設定]

```
interface   en0             */*          numbered③
interface   en1/10.0.0.1   10.0.0.0/8   numbered④
```

[本装置のippoolファイルの設定]

```
172.31.0.32   96⑤
```

[本装置のipfiltersファイルの設定]

```
%FILTER da_lan1⑥
        DA = 172.31.0.0/16
```

[本装置のusersファイルの設定]

```
%preset
        auth_request    pap
        auth_accept     none
#userAに対する設定
%user
        remote_name     userA
        remote_passwd   xxxxxxxxxxx
        interface isdn0 * unnumbered
                ppp address on * 255.255.255.254
                access include da_lan1⑦
#userBに対する設定
%user
        remote_name     userB
        remote_passwd   xxxxxxxxxxx
        interface isdn0 * unnumbered
                ppp address on * 255.255.255.254
```

[解　説]

① 本装置のホスト名を設定します。
② 本装置のホスト名とIPアドレスの対応関係を設定します。
③ 論理インタフェースen0(LAN1ポートに対応)を設定します。この例の場合、自局IPアドレスとして本装置のホスト名のIPアドレス(172.31.0.1)が、相手IPアドレス/マスクとして172.31.0.0/16が設定されたことになります。以下の設定でも同じ結果になります。

```
interface   en0/172.31.0.1   172.31.0.0/16   numbered
```

④ 論理インタフェースen1(LAN2ポートに対応)を設定します。この例の場合、自局IPアドレスとして10.0.0.1を、相手IPアドレス/マスクとして10.0.0.0/8を設定しています。
⑤ 172.31.0.32～172.31.0.127までの96個のIPアドレスをIPプールに設定しています。
⑥ ネットワーク1(172.31.0.0/16)宛てのパケットにマッチするフィルタをda_lan1フィルタとして定義しています。
⑦ 接続相手userAからの入力パケットを制限する設定をしています。この例の場合、ipfiltersファイルに定義したフィルタ「da_lan1」にマッチするパケットのみが通過します。つまり、userAはネットワーク1へのアクセスしかできないことになります。

（ここは空白のページです。）

4.5.4　LAN1ポートとLAN2ポートを使用する場合の設定(端末型接続を行う場合2)

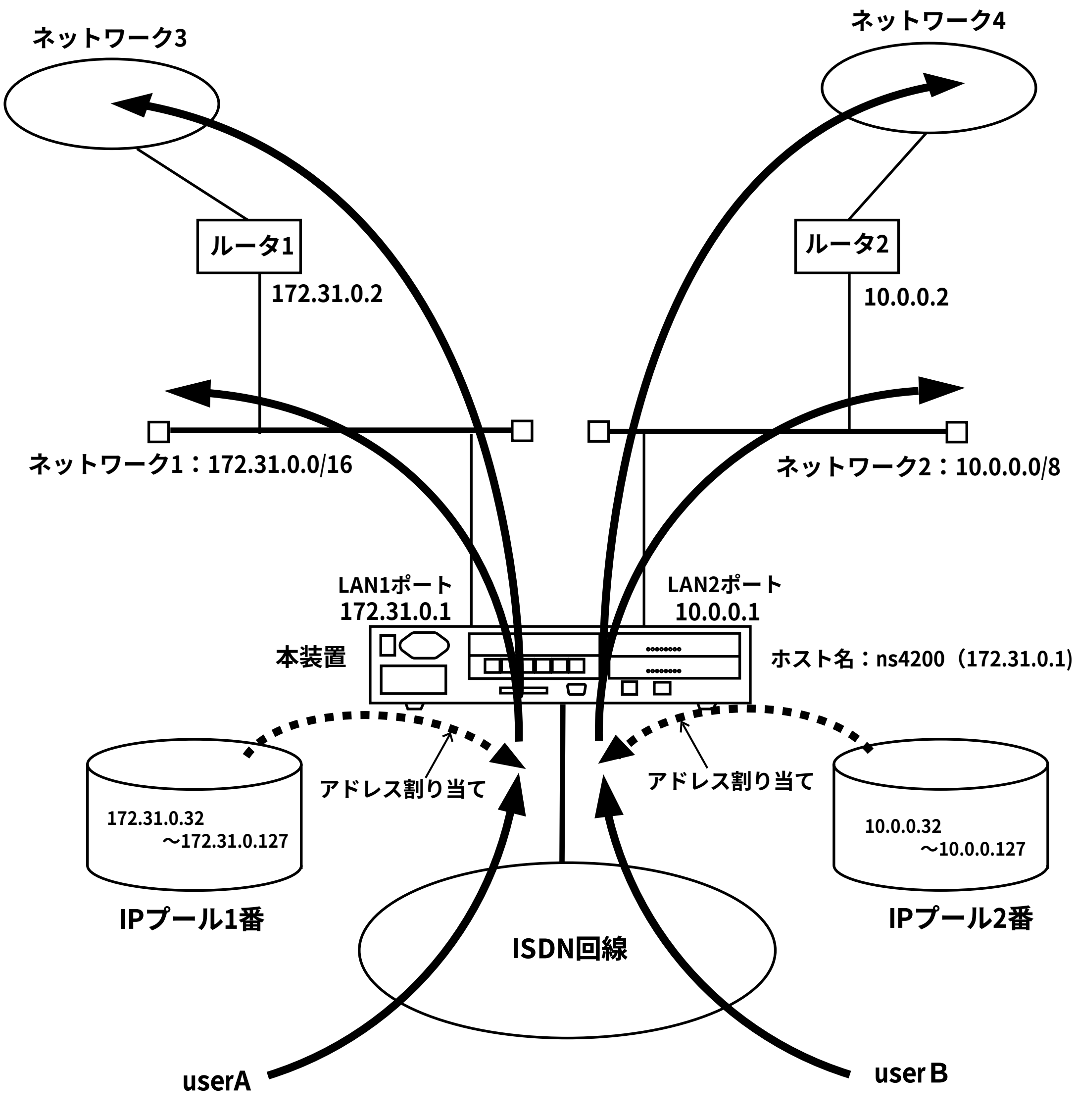
ここでは、本装置の2つのLANポートを使用し、ISDN経由で端末型接続してきた相手のユーザ名に応じてルーティングするLANポートを使い分ける場合について説明します。
以下に示す例では、

- 接続相手に割り当てるIPアドレスをLAN1ポート側ルーティング用とLAN2ポート側ルーティング用に分けてプールしておく。
- LAN1ポート側ルーティング用にプールしているIPアドレスを送信元IPアドレスとするパケットのみがLAN1ポート側にルーティングされるようにフィルタを設定しておく。
- LAN2ポート側ルーティング用にプールしているIPアドレスを送信元IPアドレスとするパケットのみがLAN2ポート側にルーティングされるようにフィルタを設定しておく。
- 接続相手毎にどのプールからIPアドレスを割り当てるかを指定しておく。

の手法を用います。

次のようなネットワーク構成を例に説明します。

- LAN1ポートをネットワーク1(ネットワークアドレス172.31.0.0/16)に接続する。
- LAN1ポートの自局IPアドレスとして172.31.0.1を使用する。
- LAN2ポートをネットワーク2(ネットワークアドレス10.0.0.0/8)に接続する。
- LAN2ポートの自局IPアドレスとして10.0.0.1を使用する。
- ネットワーク1の先には、ルータ1(172.31.0.2)経由でネットワーク3が接続されている。
- ネットワーク2の先には、ルータ2(10.0.0.2)経由でネットワーク4が接続されている。
- userA、userBからの端末型接続を受け付ける。ただし、userAはLAN1ポート側のみにルーティングし、userBはLAN2ポート側のみにルーティングする。
- 端末型接続時に割り当てるIPアドレスとして、172.31.0.32～172.31.0.127までの96個のIPアドレスと、10.0.0.32～10.0.0.127までの96個のIPアドレスを分けてプールしておく。


ネットワーク3
ネットワーク4
ルータ1
ルータ2
172.31.0.2
10.0.0.2
ネットワーク1：172.31.0.0/16
ネットワーク2：10.0.0.0/8
LAN1ポート
172.31.0.1
LAN2ポート
10.0.0.1
本装置
ホスト名：ns4200（172.31.0.1）
アドレス割り当て
アドレス割り当て
172.31.0.32
～172.31.0.127
10.0.0.32
～10.0.0.127
IPプール1番
IPプール2番
ISDN回線
userA
user B

［本装置のhostnameファイルの設定］

```
ns4200①
```

［本装置のhostsファイルの設定］

```
172.31.0.1   ns4200②
```

［本装置のinterfaceファイルの設定］

```
interface   en0            */*          numbered③
        filter   sa_pool1⑤
interface   en1/10.0.0.1   10.0.0.0/8   numbered④
        filter   sa_pool2⑥
```

［本装置のgatewaysファイルの設定］

```
destination   0.0/0   via   172.31.0.2  2
        filter   sa_pool1⑦
destination   0.0/0   via   10.0.0.2  3
        filter   sa_pool2⑧
```

［本装置のippoolファイルの設定］

```
%ippool 1⑨
        172.31.0.32   96
%ippool 2⑩
        10.0.0.32     96
```

［本装置のipfiltersファイルの設定］

```
%FILTER sa_pool1⑪
                SA = 172.31.0.32/27
        OR      SA = 172.31.0.64/26
%FILTER sa_pool2⑫
                SA = 10.0.0.32/27
        OR      SA = 10.0.0.64/26
```

［本装置のusersファイルの設定］

```
#userAに対する設定
%user
        remote_name     userA
        remote_passwd   xxxxxxxxxxx
        ippool          1⑬
        interface isdn0 * unnumbered
                ppp address on * 255.255.255.254
#userBに対する設定
%user
        remote_name     userB
        remote_passwd   xxxxxxxxxxx
        ippool          2⑭
        interface isdn0 * unnumbered
                ppp address on * 255.255.255.254
```

［解　説］

① 本装置のホスト名を設定します。

② 本装置のホスト名とIPアドレスの対応関係を設定します。

③ 論理インタフェースen0(LAN1ポートに対応)を設定します。この例の場合、自局IPアドレスとして本装置のホスト名のIPアドレス(172.31.0.1)が、相手IPアドレス/マスクとして172.31.0.0/16が設定されたことになります。以下の設定でも同じ結果になります。

```
    interface   en0/172.31.0.1   172.31.0.0/16   numbered
```

④ 論理インタフェースen1(LAN2ポートに対応)を設定します。この例の場合、自局IPアドレスとして10.0.0.1を、相手IPアドレス/マスクとして10.0.0.0/8を設定しています。

⑤ ネットワーク1へのルーティングについてフィルタを設定しています。この例の場合、ipfiltersファイルに定義したフィルタ「sa_pool1」にマッチするパケットのみがこのルーティングを使用できます。つまり、IPプールの1番からIPアドレスを割り当てられた端末はこのルーティングを使用できます。

⑥ ネットワーク2へのルーティングについてフィルタを設定しています。この例の場合、ipfiltersファイルに定義したフィルタ「sa_pool2」にマッチするパケットのみがこのルーティングを使用できます。つまり、IPプールの2番からIPアドレスを割り当てられた端末はこのルーティングを使用できます。

⑦ ネットワーク3へのルーティング(デフォルトルート)についてフィルタを設定しています。この例の場合、ipfiltersファイルに定義したフィルタ「sa_pool1」にマッチするパケットのみがこのルーティングを使用できます。つまり、IPプールの1番からIPアドレスを割り当てられた端末はこのルーティングを使用できます。

⑧ ネットワーク4へのルーティング(デフォルトルート)についてフィルタを設定しています。この例の場合、ipfiltersファイルに定義したフィルタ「sa_pool2」にマッチするパケットのみがこのルーティングを使用できます。つまり、IPプールの2番からIPアドレスを割り当てられた端末はこのルーティングを使用できます。

⑨ IPプールの1番に、172.31.0.32～172.31.0.127までの96個のIPアドレスをプールしています。
⑩ IPプールの2番に、10.0.0.32～10.0.0.127までの96個のIPアドレスをプールしています。
⑪ IPプールの1番にプールされているIPアドレスを送信元アドレスとするパケットにマッチするフィルタをsa_pool1として定義しています。172.31.0.32/27で172.31.0.32～172.31.0.63までのアドレスをマッチさせています。172.31.0.64/26で172.31.0.64～172.31.0.127までのアドレスをマッチさせています。
⑫ IPプールの2番にプールされているIPアドレスを送信元アドレスとするパケットにマッチするフィルタをsa_pool2として定義しています。10.0.0.32/27で10.0.0.32～10.0.0.63までのアドレスをマッチさせています。10.0.0.64/26で10.0.0.64～10.0.0.127までのアドレスをマッチさせています。
⑬ userAには、IPプールの1番からIPアドレスを割り当てるようにします。
⑭ userBには、IPプールの2番からIPアドレスを割り当てるようにします。

注　意　**本装置自身が送信するパケットにはIPフィルタがかかりません。この例では2つのデフォルトルートを設定していますが、本装置自身が使用するデフォルトルートはメトリックの低い方（ルータ1へのルート）になります。**

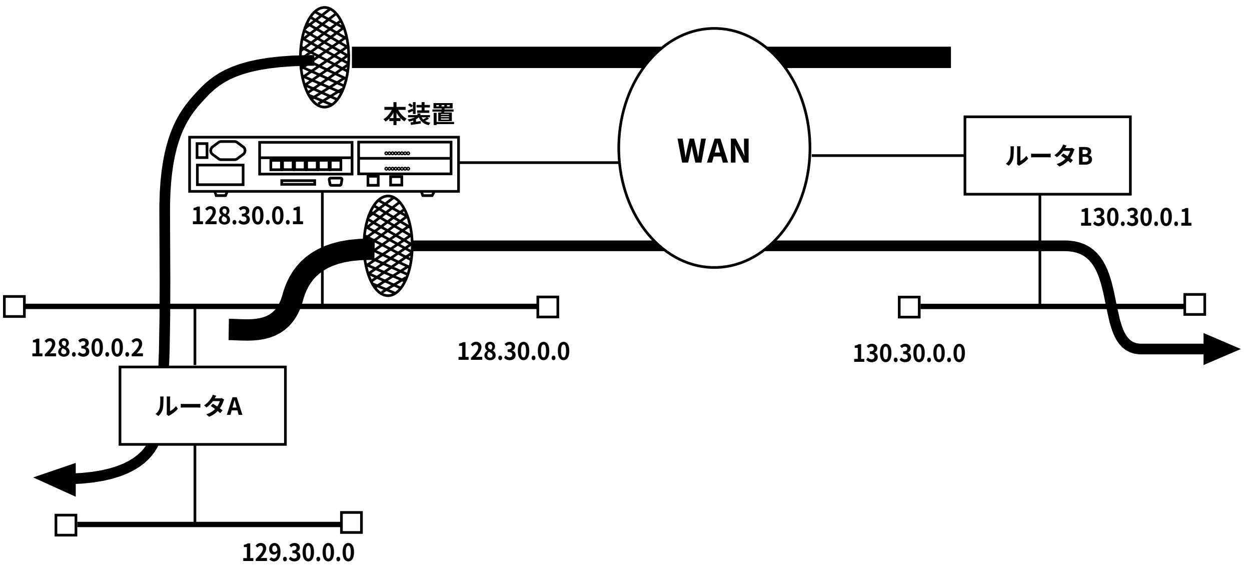
4.6　その他の機能の設定

4.6.1　IPフィルタ機能を使用する場合の設定

本装置は、特定のルートに対してパケットを選別するためのフィルタ（単にフィルタと呼びます）と、インタフェースからの入力パケットを選別するフィルタ（アクセスリストと呼びます）と、インタフェースへの出力パケットを選別するフィルタ（アウトプットフィルタと呼びます）を設定することができます。

(1) フィルタ

ある特定のルートに対してフィルタを設定することができます。したがってフォワーディングされるパケットを通したり、廃棄したりできます。
特定のパケットを通すフィルタは、該当するルートにフィルタの指定をします。
特定のパケットを廃棄するためのフィルタは、該当するルートとnoforwardを経由するルートとを組み合わせて設定します。noforwardを経由するルートに廃棄したいパケットのフィルタを指定します。
noforwardは、本装置内の仮想ルータで、あらかじめhostsファイルに登録されているホスト名です。このnoforwardを経由しようとするパケットは、すべて廃棄されます。したがって、noforwardを経由するルートに廃棄したいパケットのフィルタを指定し、かつ、メトリックを小さくしておけば、このフィルタ条件に合ったルートへのパケットは廃棄され、他のパケットは、このnoforwardのルートの条件に合わないので該当するルートを通過します。



■WAN側ルートへのフィルタ（usersファイル）

WAN側のルートへのフィルタは、usersファイルに設定します。

特定のパケットを通すフィルタ

```
destination 130.30.0.0/16 via 130.30.0.1  2
       filter telnetFIL
```

この例では、130.30.0.0のネットワークへフォワーディングされるパケットのうち、telnetFIL（telnetを通す）の条件を満たしたパケットのみ通過します。

特定のパケットを廃棄するフィルタ

usersファイル

```
destination 130.30.0.0/16 via 130.30.0.1  2
```

gatewaysファイル

```
destination 130.30.0.0/16 via noforward   1
       filter telnetFIL
```

この例では、130.30.0.0のネットワークへフォワーディングされるパケットのうち、telnetFIL（telnetを通す）の条件を満たしたパケットは、noforward経由になり廃棄されます。条件に合わないパケット、つまりtelnet以外のパケットは、130.30.0.0のネットワークへフォワーディングされます。

注 意　noforward経由でパケットを廃棄するルートは、必ずgatewaysファイルに指定してください。

■LAN側ルートへのフィルタ（gatewaysファイル）

LAN側のルートへのフィルタは、gatewaysファイルに設定します。

特定のパケットを通すフィルタ

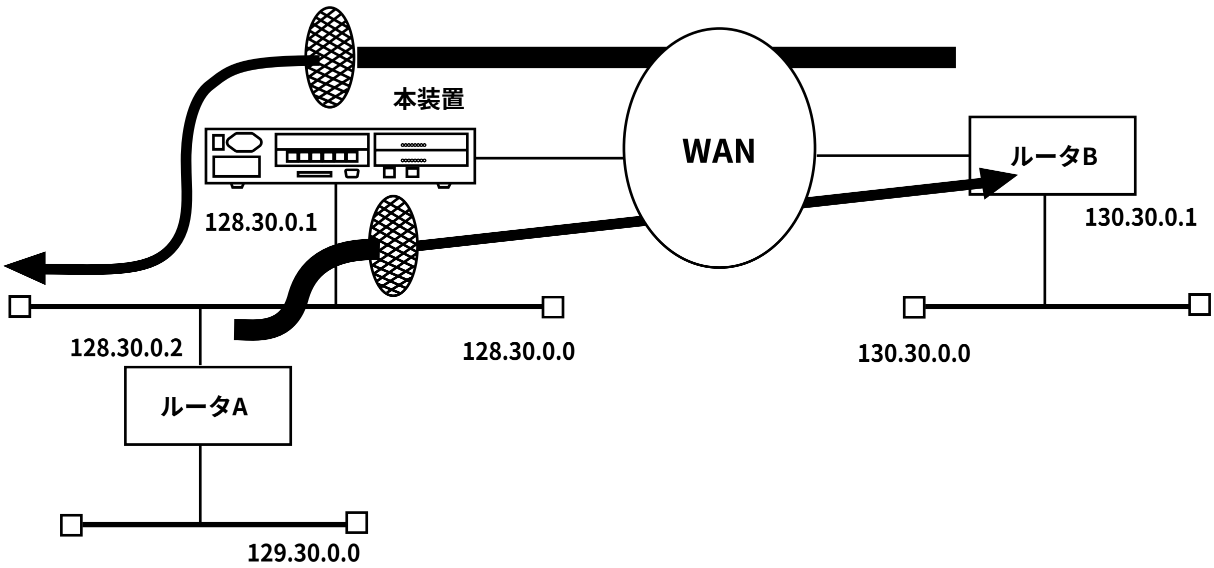
```
destination 129.30.0.0/16 via 128.30.0.2  2
       filter telnetFIL
```

特定のパケットを廃棄するフィルタ

```
destination 129.30.0.0/16 via 128.30.0.2  2
destination 129.30.0.0/16 via noforward   1
       filter telnetFIL
```

■直結するセグメント宛てのフィルタ

直結するセグメント宛てのパケットに対して通すフィルタを設定できます。



WAN側のフィルタ（usersファイル）

下記の例のように、130.30.0.1のホスト宛てのパケットにフィルタをかけたい場合、destinationの設定の部分のフィルタでは、フィルタリングされません。このような場合には、interfaceの設定の部分にフィルタの指定を行ってください。

特定のパケットを通すフィルタ

```
interface isdn0 130.30.0.1 unnumbered
       filter telnetFIL
destination 130.30.0.0/16 via 130.30.0.1 2
       filter telnetFIL
```

LAN側のフィルタ（interfaceファイル）

LANに直結するセグメント宛てのパケットに対するフィルタは、interfaceファイルで設定します。

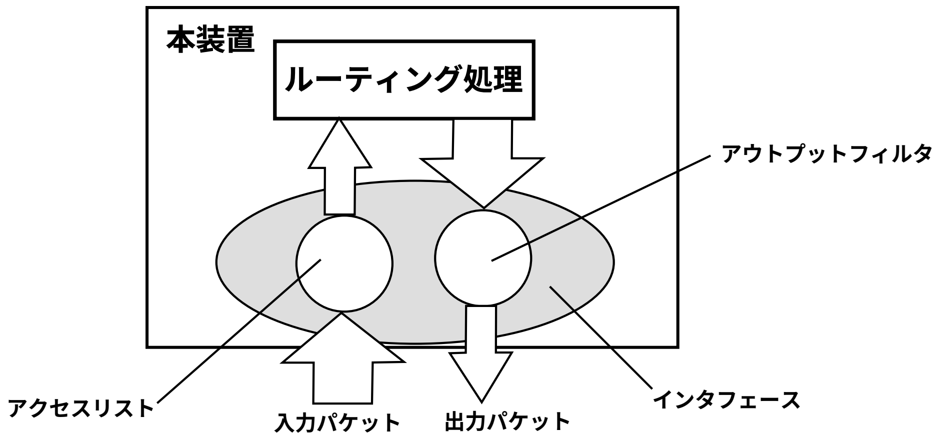
特定のパケットを通すフィルタ

```
interface en0 */* unnumbered
       filter telnetFIL
```

(2) アクセスリストとアウトプットフィルタ

アクセスリストは、各インタフェースで入力パケットのフィルタリングをする機能です。一方、アウトプットフィルタは、各インタフェースで出力パケットのフィルタリングをする機能です。この機能を用いて、各インタフェースの入力パケットを制限したり、出力を許可するパケットを制限することができます。フィルタの条件には、IPアドレス、プロトコル、ポート番号、TOS、入力インタフェースなどを指定でき、さらにANDやOR演算を使用してきめ細かな条件設定が可能です。

本装置へのパケット入力は、各インタフェースから行われます。この入力時に働くフィルタがアクセスリストです。アクセスリストを通過したパケットは、本装置内でルーティング処理が行われ、出力インタフェースが決定されます。出力インタフェースに出力する際に働くフィルタがアウトプットフィルタです。アウトプットフィルタを通過したパケットのみがインタフェースに出力されます。



アクセスリストにより、本装置自身にtelnetでログインできる発信元IPアドレスを制限したり、発信元IPアドレスのフィルタを設定して、なりすましパケットの入力を防ぐことができます。また、アウトプットフィルタにより特定のインタフェースへの出力パケットは、FTPとメイルのみに限定するなどの制限を設けられます。

特　徴

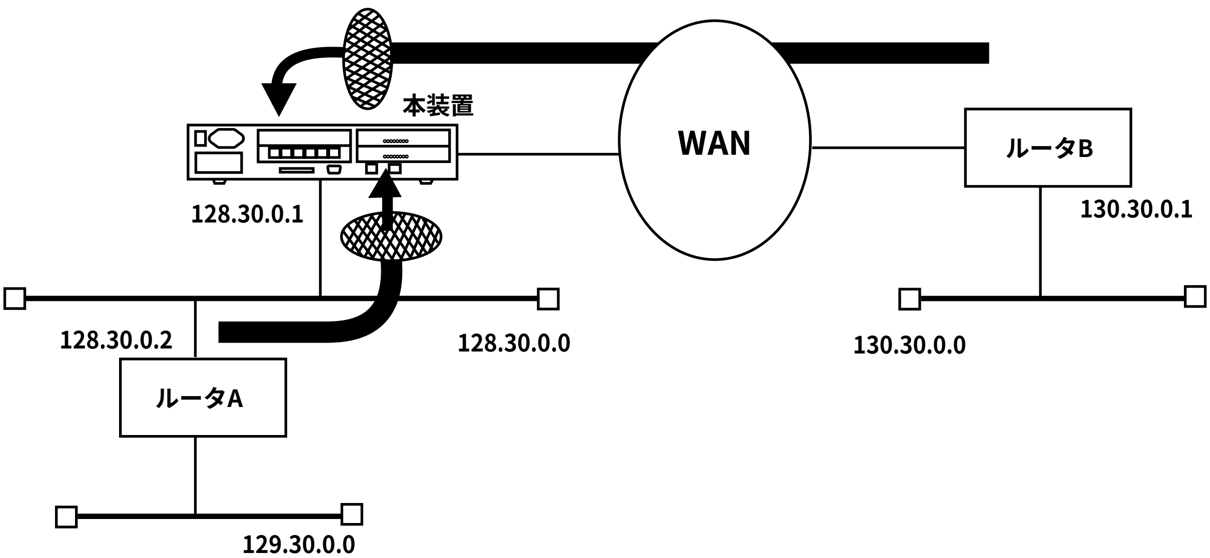
- インタフェースごとにフィルタ条件を指定可能
- 入力と出力に異なるフィルタ条件を指定可能
- フィルタ条件に、発信元IPアドレス、宛先IPアドレス、プロトコル、発信元ポート番号、宛先ポート番号、TOS、入力インタフェースを指定可能
- フィルタ条件として、各項目の一致／不一致を指定可能
- 各条件のAND／OR演算が可能
- 発信元IPアドレス、宛先IPアドレスには、特定ホストアドレスやネットワークアドレスの指定が可能。ポート番号には大小比較が指定可能
- 高速なフィルタリング処理を実現
- フィルタの統計情報をコマンド(netstat -fil)で採取可能

①アクセスリスト

アクセスリストは、IPパケットの入力フィルタ機能です。インタフェースごとに入力フィルタの設定ができます。
アクセスリストの処理は、IPのパケット受信処理中に行われるため、廃棄されたパケットは、どんな経路にもフォワーディングされません。
また、本装置自身宛てのパケットも同様に廃棄されるため、セキュリティ確保に用いることが可能です。

```
interface  <インタフェース名>・・・・・
        access {include | exclude}  <フィルタ名>
```

<フィルタ名>のフィルタを通過するパケットのみを有効にし、それ以外のパケットを廃棄したい場合、includeを指定します。逆に、廃棄したいパケットをフィルタで指定する場合には、excludeを指定します。



■WAN側のアクセスリスト（usersファイル）

WAN側のアクセスリストは、usersファイルに設定します。

特定のパケットを通すアクセスリスト

```
interface isdn0 130.30.0.1 unnumbered
      access include telnetFIL
```

特定のパケットを廃棄するアクセスリスト

```
interface isdn0 130.30.0.1 unnumbered
      access exclude telnetFIL
```

■LAN側のアクセスリスト（interfaceファイル）

LAN側のアクセスリストは、interfaceファイルに設定します。

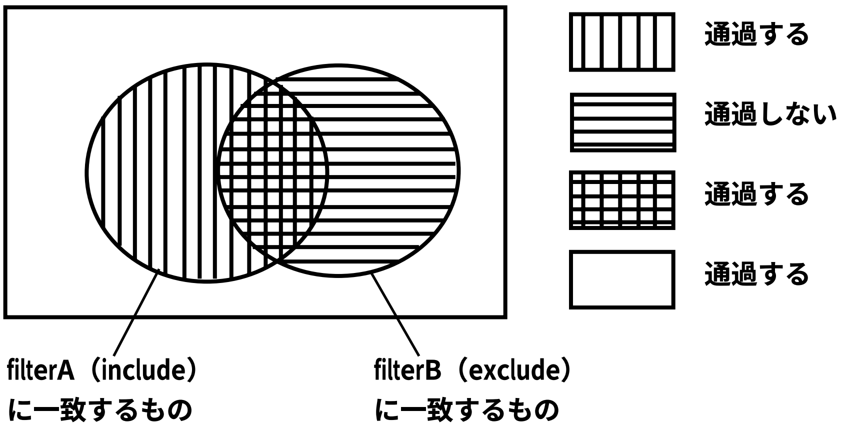
特定のパケットを通すアクセスリスト

```
interface en0 */* numbered
      access include telnetFIL
```

特定のパケットを廃棄するアクセスリスト

```
interface en0 */* numbered
      access exclude telnetFIL
```

1つのインタフェースに対して、include、excludeを同時に設定することができます。両方を設定した場合にも、includeで指定したフィルタに一致するものは通過し、excludeで指定したフィルタに一致するものは廃棄するという基本的な考え方は変更ありません。
ただし、includeのフィルタにもexcludeのフィルタにも一致した場合には、includeが優先され「通過する」となります。また、includeのフィルタにもexcludeのフィルタにも一致しない場合には、excludeが優先され「通過する」となります。



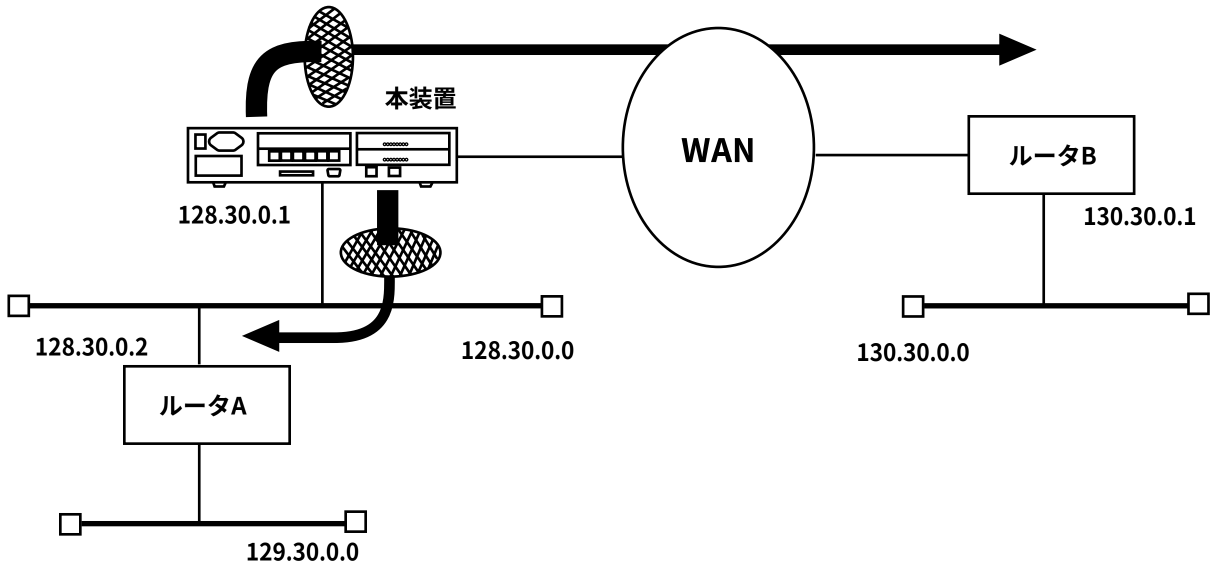
通常のフィルタの使い方としては、includeまたはexcludeのどちらか一方を指定してください。

②アウトプットフィルタ

アウトプットフィルタは、IPパケットの出力フィルタ機能です。
インタフェースごとに異なるフィルタを設定できます。
あるインタフェースへの出力パケットプロトコルを制限したり、ポート番号を制限して不正アクセスパケットの流出を防ぐことができます。

```
interface <インタフェース名>・・・・・
       outputfil <フィルタ名>
```

アウトプットフィルタが設定されたインタフェースからは、<フィルタ名>のフィルタを通過するパケットのみが出力されます。



■WAN側のアウトプットフィルタ(usersファイル)

WAN側のアウトプットフィルタは、usersファイルに設定します。

アウトプットフィルタの例

```
interface isdn0 130.30.0.1 unnumbered
       outputfil telnetFIL
```

■LAN側のアウトプットフィルタ(interfaceファイル)

LAN側のアウトプットフィルタは、interfaceファイルに設定します。

アウトプットフィルタの例

```
interface en0 */* numbered
       outputfil telnetFIL
```

(3) フィルタ条件の定義

フィルタの条件は、ipfiltersファイルに設定します。
ひとつのIPフィルタは、OR条件で結合された1つ以上のIPフィルタエントリから構成されます。各IPフィルタエントリは、IPヘッダ中の、宛先IPアドレス、発信元IPアドレス、上位層プロトコル識別子、サービス種別の各フィールドおよびIPヘッダ直後の2バイト、さらにその後の2バイト(通常、トランスポート層の発信元ポート番号と宛先ポート番号に相当)で構成され、各フィールドごとに指定、無視(DON'T CARE)を設定できます。

X X X X	**発信元アドレス =129.30.0.1**	X X X X

OR

X X X X	X X X X	**宛先アドレス =128.30.0.2**

■ipfiltersファイルのセットアップ

ipfiltersファイルは、gatewaysファイル、interfaceファイル、usersファイルで指定するフィルタの定義を行うためのセットアップです。
各IPフィルタは、%FILTERキーワードを使って定義します。

```
%FILTER <フィルタ名-1>
        <フィルタ本体行-1>
              •
              •
        <フィルタ本体行-n>
%FILTER <フィルタ名-2>
        <フィルタ本体行-1>
              •
              •
        <フィルタ本体行-N>
              •
              •
%FILTER<フィルタ名-N>
        <フィルタ本体行-1>
              •
              •
        <フィルタ本体行-N>
```

%FILTERキーワードの行以降、次の%で始まるキーワードの行またはファイルの最後までが、1つのIPフィルタの定義です。
フィルタ本体行は、1つ以上のフィルタエントリを予約語ORで連結して表現します。ただし、ipfiltersファイルの中での改行は、語の区切りの意味しか持たないため、空白のかわりに改行しても同じ効果となります。また各予約語は、大文字または小文字で記述できますが混在はできません。

```
%FILTER    <フィルタ名>
  <フィルタエントリ-1> OR <フィルタエントリ-2>....
%FILTER    <フィルタ名>
  <フィルタエントリ-1> OR <フィルタエントリ-2>....
```

各フィルタエントリは、そのフィールドを指定する予約語と定数の組を予約語ANDで連結して表現します。

```
%FILTER    <フィルタ名>
   SA=128.30.0.1 AND DA=0x801e002 AND PROTO=TCP
or sa=128.30.0.2 and da=yuka and proto=UDP
```

フィールドの指定のための予約語を以下に記述します。

SA(sa)	：発信元IPアドレス
DA(da)	：宛先IPアドレス
PROTO(proto)	：上位層プロトコル識別子
TOS(tos)	：サービス種別
SPORT(sport)	：IPヘッダの次の2バイト(TCPやUDPでは発信元ポート番号)
DPORT(dport)	：IPヘッダの次の2バイト(TCPやUDPでは宛先ポート番号)
INTERFACE (interface)	：そのパケットが受信されたインタフェース名

フィールドの値を指定するための定義には、%CONSTキーワードを用いて参照する行より前で定義した名前、0xまたは、0Xを先頭においた16進数、10進数、ドット記法、hostsファイルあるいはservicesファイル中で定義されている名前を使用できます。

以下、主なフィルタの構成例を記述します。これらの例の中で一般的な設定は、あらかじめipfiltersファイルに設定されています。本装置のshowコマンドを用いて確認してください。

プロトコル識別子の定義

```
%CONST
       ICMP=1
       TCP=6
       UDP=17
```

ICMPプロトコルもしくはtelnetのみ通過

```
%FILTER   telnetFIL
       proto=ICMP
   OR  proto=TCP AND SPORT=telnet
   OR  proto=TCP AND DPORT=telnet
```

ICMPプロトコルもしくはftpのみ通過

```
%FILTER   ftpFIL
       proto=ICMP
   OR  proto=TCP AND SPORT=ftp
   OR  proto=TCP AND SPORT=ftp-data
   OR  proto=TCP AND DRORT=ftp
   OR  proto=TCP AND DRORT=ftp-data
```

特定のホストグループの送信フレームのみを通過

```
%FILTER    user1FIL
       SA=yuka
   OR  SA=momo
   OR  SA=kyon
```

特定の2者間のフレームのみを通過

```
%FILTER   betweenFIL
      SA=yuka AND DA=kyon
   OR SA=kyon AND DA=yuka
```

受信インタフェースの使用例

```
%FILTER  EX1
      INTERFACE = en0 AND PROTO = TCP
   OR INTERFACE = en0 AND PROTO = UDP
```

このフィルタは、en0から受信されたTCPのパケットもしくはen0から受信されたUDPのパケットを選別します。

ビットマスク指定の例

```
%FILTER EX2
      SA = 128.30.1.16/28
   OR DA = 128.30.3.0/255.255.255.0
```

この例では、IPソースアドレスが、128.30.1.16 ～ 128.30.1.31の範囲に属するパケットもしくはIPデスティネーションアドレスが128.30.3.0 ～ 128.30.3.255の範囲に属するパケットを選別します。

ポート番号の大小比較

```
%FILTER EX3
     PROTO=TCP AND DPORT<1024 AND DPORT !=23
```

この例では、プロトコルがTCPで、宛先ポート番号が1024未満で、宛先ポート番号23を除くパケットを選別します。
使用可能な演算子を以下に示します。

表4-4　演算子一覧

演算子	意　味	使用可能な項目
=	一致	発信元IPアドレス、宛先IPアドレス、プロトコル、発信元ポート番号、宛先ポート番号、TOS、入力インタフェース
!=	不一致	発信元IPアドレス、宛先IPアドレス、プロトコル、発信元ポート番号、宛先ポート番号、TOS、入力インタフェース
<	より小さい	発信元ポート番号、宛先ポート番号
>	より大きい	発信元ポート番号、宛先ポート番号

(4) フィルタの注意および制限

① IPフィルタ(gatewaysファイル/interfaceファイル/usersファイルのfilter行で指定したもの)は、フォワーディングに関してのみ有効です。したがって、本装置自身の通信には影響しません。

② 仮想ルータnoforwardは、フォワーディングに関してのみ有効です。したがって、本装置自身のパケットは、noforwardを経由しないため廃棄されません。

③ IP-optionを含むIPフレームは、IPフィルタとnoforwardを無視し、本装置自身のパケットと同様にルーティングされます。

④ IPのフラグメンテーションが行われると、2番目以降のパケットには、SPORT, DPORTに相当する部分が含まれません。本装置は、いくつかのフラグメント情報を一定時間保持しているため、このフラグメント情報が残っている場合は、1番目のフラグメントを再生してフィルタリングを行います。残っていない場合は、IPフィルタとnoforwardを無視し、本装置自身のパケットと同様にルーティングされます。

⑤ TCPやUDPでは、SPORT、DPORTで参照されるIPヘッダの直後の2バイトおよびその後の2バイトは、それぞれ送信元ポート番号、宛先ポート番号です。TCP、UDP以外のプロトコルでSPORT、DPORTを指定しないでください。

(5) アクセスリストとアウトプットフィルタの注意および制限

① アウトプットフィルタは、フォワーディングパケットに関してのみ有効です。
本装置が送信するパケットには影響しません。

② IP-Optionを含むIPフレームは、アウトプットフィルタは無視されて出力されます。

③ IPのフラグメンテーションが行われると、2番目以降のパケットにはSPORT、DPORTに相当する部分が含まれていません。
本装置は、いくつかのフラグメント情報を一定時間保持しているため、このフラグメント情報が残っている場合には、1番目のフラグメントによりフィルタリングを行います。
残っていない場合には、アウトプットフィルタは無視されて、パケットはフィルタを通過します。

④ TCPやUDPでは、SPORT、DPORTで参照されるIPヘッダの直後の2バイトおよびその後の2バイトは、それぞれ送信元ポート番号、宛先ポート番号です。
TCP、UDP以外のプロトコルではSPORT、DPORTは指定しないでください。

4.6.2　サブネットマスクを使用する場合の設定

■LAN上のサブネット

LAN上でサブネットを使用する場合には、interfaceファイルの「en0, en1」のインタフェースに設定します。
工場出荷状態では、サブネットを使用する設定にはなっていません。サブネットを使用する場合は、必ず以下の設定をしてください。

```
interface en0/128.30.1.1 128.30.1.0/24 numbered
```

自局IPアドレス　　**LANのネットワークアドレス**　　**LANのマスク**

自局IPアドレス：
自局IPアドレスを指定します。

LANのネットワークアドレス：
LANのネットワークアドレスをサブネットの部分を含んで指定します。

LANのマスク：
LANのサブネットマスクを設定します。以下のフォーマットで指定できます。

/n	：マスクのビット長を10進数で指定します。 （例：/24）
/ddd.ddd.ddd.ddd	：ドットで区切られた10進数で指定します。 （例：/255.255.255.0）

■LAN側ルートのサブネット

LANのルートにサブネットを使用する場合には、gatewaysファイルで宛先アドレスにサブネットの指定をします。

```
destination 128.30.2.0/24 via 128.30.1.2  1
```

宛先アドレス　　**マスク**

宛先アドレス：
宛先のネットワークアドレスをサブネットの部分を含んでを指定します。

マスク：
サブネットマスクを設定します。以下のフォーマットで指定できます。

/n	：マスクのビット長を10進数で指定します。 （例：/24）
/ddd.ddd.ddd.ddd	：ドットで区切られた10進数で指定します。 （例：/255.255.255.0）

■WAN側ルートのサブネット

WANのルートにサブネットを使用する場合には、usersファイルで宛先アドレスにサブネットの指定をします。指定方法はgatewaysファイルと同様です。

4.6.3 SNMP機能の設定

■概　要

SNMP（Simple Network Management Protocol）は、ネットワーク上の装置を監視するための標準プロトコルです。SNMPを使ってネットワーク上の各装置を管理する側をSNMPマネージャと呼び、管理される側をSNMPエージェントと呼びます。本装置はSNMPエージェント機能を備えています。

本装置のSNMPエージェントは、以下の機能をサポートしています。

・SNMP（RFC1157）プロトコルをサポートしています。
・MIB2（RFC1213）をサポートしています。
　MIB2で規定されている各種インタフェースの統計情報を取り出すことができます。
・認証違反などの不正アクセスなどをトラップとしてマネージャに知らせる機能をサポートしています。
・コミュニティやビューによりマネージャからのアクセス制限を設定することができます。
・ユーザによる各種項目のコンフィグレーションが可能です。

■セットアップ

SNMPエージェント機能の設定は、snmpconfファイルに行います。設定内容としては、アクセスを許可するコミュニティ名の設定や、トラップの送信先ホスト、トラップの条件などの設定ができます。

snmpconfファイルの設定例

```
#
# Basic Configuration
sysContact    "Yatanabe 777-7777"   連絡先
sysLocation   "System Design.G 3F"  設置場所
community     public view1          コミュニティ名とビュー
#
# Trap Configuration
trap   snmpmgr       public         トラップの送信先ホストとコミュニティ名1
trap   backmgr       public         トラップの送信先ホストとコミュニティ名2
linkTrap     on                     リンクUp/Downトラップを送信する
linktrapifs  en0 en1                リンク Up/Down 監視インタフェース
```

4章 各種機能の設定方法

(1) 基本設定

基本設定には各装置の管理者の名前や設置場所などを設定します。また、アクセスを許可するコミュニティ名とビューを設定します。

SNMPの基本設定

```
# Basic Configuration
sysContact    “Yatanabe 777-7777”       連絡先
sysLocation   “System Design.G 3F”      設置場所
community     public view1              コミュニティ名とビュー
```

sysContact ：この装置の管理者の名前や所属、電話番号などの情報を文字列で設定します。文字列は「“」でくくって設定します。

sysLocation ：この装置の設置場所の情報を文字列で設定します。
文字列は「“」でくくって設定します。

community ：アクセスを許可するコミュニティ名と、そのビューを設定します。
コミュニティ名にはそのコミュニティ名か「*」を設定します。
「*」は、すべてのコミュニティ名を意味します。
ビューは、リードのみ許可する場合には「view1」を指定します。リード／ライトの両方を許可する場合には、「view2」を指定します。
この例では、コミュニティpublicからのリードアクセスを許可しています。
また、アクセスを認めるSNMPマネージャのIPアドレスを指定することができます。そのための記述例を以下に示します。

```
community   public   view1   172.16.1.1
```

この例では、コミュニティ名がpublicで、IPアドレスが172.16.1.1であるマネージャからのリードアクセスを許可しています。

注 意　　コミュニティ名は最大20 個まで設定できます。

(2) トラップの設定

トラップの設定には、トラップの宛先のSNMPマネージャの設定、Authentication違反トラップの設定、リンクのアップ／ダウントラップの設定などがあります。

SNMPのトラップに関する設定

```
# Trap Configuration
trap   snmpmgr       public   ――― トラップの送信先ホストとコミュニティ名1
trap   backmgr       public   ――― トラップの送信先ホストとコミュニティ名2
authenTrap           on       ――― 認証違反のトラップを送信する
linkTrap             on       ――― リンクUp/Downトラップを送信する
linktrapifs en0 en1                        ┐
linktrapifs P1-1PRI P1-2PRI P1-3PRI        ├― リンクUp/Down監視インタフェース
linktrapifs hsd1 hsd2 hsd3                 ┘
```

trap ：SNMPトラップの送信先のホストおよびコミュニティ名と、トラップの送信元IPアドレスを設定します。
送信先のホストはIPアドレスまたはhostsファイルに設定したホスト名で指定できます。
コミュニティ名を省略した場合には、コミュニティ名を含まないトラップが送信されます。
送信元IPアドレスを省略した場合には、本装置のホスト名に対応したIPアドレスが使われます。
送信元IPアドレスを設定した場合の例を以下に示します。

```
trap   snmpmgr   public   172.16.1.100
```

この例では、送信先がsnmpmgr、コミュニティ名がpublic、送信元IPアドレスが172.16.1.100です。

注 意
- **トラップの送信先は最大20個まで設定できます。**
- **送信元IPアドレスは、interfaceファイルなどで、本装置のIPアドレスとして、あらかじめ設定されている必要があります。**

authenTrap ：Authentication違反トラップを送信するか設定します。
トラップを送信させたい場合には、「on」を指定します。
この項目を省略した場合には、デフォルトで「off」になります。

linkTrap ：linkUp/Downトラップを送信するか設定します。
トラップを送信させたい場合には、「on」を指定します。
この項目を省略した場合には、デフォルトで「off」になります。

linktrapifs ：リンクのUp/Downを検出したらトラップを発生させる論理インタフェース名を設定します。
「en0, en1」はそれぞれLAN1、LAN2ポートを表します。
「P1-1PRI, P1-2PRI, P1-3PRI」は、それぞれ拡張ボードスロット1のPRIポート1、2、3を表します。
「hsd1, hsd2, hsd3」は、それぞれ高速ディジタル回線の論理インタフェース名を表します。

注 意　　本装置のSNMPエージェントはトラップの頻発を防ぐため定期的に状態を監視しています。もし、監視の間隔の間にUp→Down→Upと状態が変化した場合にはトラップは発生しません。

■SNMP機能の起動

SNMPを起動するには、serversファイルの/share/snmpdの行の先頭の「#」を削除します。その後、本装置をリブートするか、またはsnmprestartコマンドを実行すると、SNMPが立ち上がります。

serversファイルの設定例

```
 :
# SNMP
#/share/snmpd     # SNMP agent
```

この#を削除する

4.6.4　ドメインネームシステムの設定

(1) 概　要

ドメインネームシステム（以後、DNSと呼びます）は、インターネット上のホストを識別するための階層形式の名前付けシステムが入った分散型データベースを提供します。DNSの仕様は、RFC1034とRFC1035で定義されています。
DNSデータベースは、ドメインネームスペースと呼ばれるツリー構造になっていて、各ホストやドメインには名前がついています。インターネットのドメインネームスペースは、最上位のドメイン名はNIC（Network Information Center）が管理し、それ以下のサブドメイン名は分散的に管理されています。
ドメイン名は、ドメインネームスペースのなかの位置を表しています。それぞれのドメインの名前をドット「.」で区切って指定します。例えば、日本のドメイン名でよく使われる「co.jp」は、親ドメインが「jp」であるサブドメイン「co」を表します。
DNSには、クライアント／サーバモデルが使われています。ネームサーバは、ゾーンと呼ばれるドメインネームスペースのなかのある一定範囲を管理します。リゾルバは、ネームサーバにホスト名とIPアドレスとの変換を問い合わせるクライアントです。

本装置では、リゾルバのみをサポートしています。DNSを使用する場合には、他のホスト上でネームサーバを設定し起動しておかなければなりません。
本装置でリゾルバを使用する設定を行うと、ホスト名を使うアプリケーション、例えばtelnetコマンドでホスト名を使用する場合や、ipfiltersファイルでホスト名をフィルタの条件に加えた場合等に自動的にDNSサーバへの問い合わせが行われます。

(2) 設　定

本装置でDNSリゾルバを使用する場合には、必要な情報をresolv.confファイルに設定します。

resolv.confファイルの設定例

```
#
domain        xxx.co.jp
nameserver    128.30.0.3
nameserver    128.30.0.4
```

domain　：ホスト名の最後にドット「.」が付いていない名前に付加されるドメイン名を指定します。

nameserver　：問い合わせるネームサーバのIPアドレスをドット表記で指定します。
最大3個までのネームサーバの対を記述できます。
最初のネームサーバへの問い合わせがタイムアウトすると順に次のネームサーバに問い合わせます。

本装置の名前からIPアドレスへの変換は、最初にhostsファイルを検索します。ここで指定された名前がない場合、resov.confファイルが設定されていれば、DNSネームサーバに問い合わせます。

(3) 注意事項

本装置のホスト名に対するIPアドレスは、必ずhostsファイルに指定してください。
リゾルバの設定をして本装置をブートする場合、DNSネームサーバが起動していないと、ネームサーバへの問い合わせでタイムアウトが発生し、ブートに異常に時間がかかることがあります。本装置の設定のなかでホスト名を使用する場合には、そのホスト名とIPアドレスをhostsファイルに指定してください。

（ここは空白のページです。）

4.6.5 ダイナミックルーティングの設定

■概　要

本装置は、ダイナミックルーティングの機能としてRIP(Routing Information Protocol)バージョン1、バージョン2をサポートしています。RIPとはルータから送信されるルーティング情報(RIPパケット)によってルーティングテーブルを自動的に更新する機能です。
この機能はRFC1058、RFC1723に準拠しています。
本装置は、LAN側や高速ディジタル回線側のルータやホストとルーティング情報を交換することができますが、ISDN回線にRIPによるルーティング情報は送信しません。ISDN回線から受信したルーティング情報も廃棄します。
ISDN側のリモートネットワークについてのルーティング情報は、設定によりLAN側(ローカルネットワーク)や高速ディジタル回線側に広告することができます。

■セットアップ

(1) routed起動の設定(serversファイル)

ダイナミックルーティングの機能は、routedと呼ばれるサーバによって実行されます。この機能を使用するには、ブート時にroutedを立ち上げるように、serversファイルに設定します。出荷時にはroutedが動作しない設定になっています。動作させるには、serversファイルを以下のように変更し、リブートしてください。

出荷時のserversファイル

```
#/share/routed
```

serversファイルの修正例

```
/share/routed
```

──── **コメント「#」を外す。**

(2) RIPの設定(rip.confファイル)

RIPの設定はrip.confファイルに行います。rip.confファイルの変更内容はreloadコマンドを実行すると有効になります。
設定には、インタフェース毎の設定と広告するルートの設定があります。インタフェース毎に設定できる項目は、送受信の制御、認証の設定があります。広告するルートの設定は、ISDN側のルートやデフォルトルートを広告する場合に設定します。

rip.confファイルの設定例

```
interface      en0        ――――――――――― 論理インタフェース名の設定
        in     rip2       ――――――――――― 受信の制御
        out    rip2       ――――――――――― 送信の制御
        auth   passwd     ――――――――― 認証の設定
        passwd makuhari   ――――――――― パスワードの設定

destination  172.31.0.0/16  via 172.30.1.1  2 ┐
destination  0.0/0 10                         ┘ 広告するルートの設定
```

interface ：論理インタフェース名を指定します。指定しないインタフェースからRIPパケットを受信した場合は、そのパケットを廃棄します。

論理インタフェース名	説　　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
hsd∗	高速ディジタル回線の論理インタフェース名（∗：1〜）

in ：受信の制御方法を指定します。

rip1 ：RIP1パケットのみを受信します。
rip2 ：RIP2パケットのみを受信します。
both ：RIP1、RIP2の両方のパケットを受信します。(デフォルト)
none ：RIPパケットを廃棄します。

out ：送信の制御方法を指定します。

rip1 ：RIP1パケットをブロードキャストで送信します。(デフォルト)
rip2 ：RIP2パケットをブロードキャストで送信します。
rip2mcast ：RIP2パケットをマルチキャストで送信します。マルチキャストアドレスは224.0.0.9です。
none ：RIPパケットを送信しません。

auth ：認証方法を指定します。

passwd ：認証をシンプルパスワードで行います。
none ：認証を行いません。(デフォルト)

passwd ：パスワードを設定します。パスワードは英数字で最大16文字です。

destination ：広告するルートを設定します。書式は以下のとおりです。

destination <宛先アドレス>/<マスク> [via <経由ルータ>] <メトリック>

<宛先アドレス> ：デスティネーションのネットワークアドレス、またはホストアドレスを設定します。

<マスク> ：<宛先アドレス>に対するマスクのビット長を10進数で設定します。デフォルトルートを設定する場合には、<宛先アドレス>/<マスク>を「0.0/0」と設定してください。

<経由ルータ> ：パケットをフォワーディングするルータの<IPアドレス>を指定します。ダイアルアップ先のルートを広告する場合には、省略します。

<メトリック> ：このルートのメトリックを10進数で設定します。範囲は1から15です。

注　意　**認証の設定はRIP2の場合に有効になります。**

注　意　**認証を行う設定の場合には、RIP1パケットと認証が成功したRIP2パケットを受け入れます。RIP1パケットを廃棄したい場合には、受信の制御で「rip2」を指定してください。**

注　意　**認証を行わない設定の場合には、RIP1パケットと認証の付いていないRIP2パケットを受け入れます。認証の付いたRIP2パケットは廃棄します。**

（ここは空白のページです。）

■構成例

以下のネットワーク構成を例にrip.confファイルの設定を説明します。

(1) ISDN側のルートを広告する場合の設定(接続相手にIPアドレスを割り当てる場合)

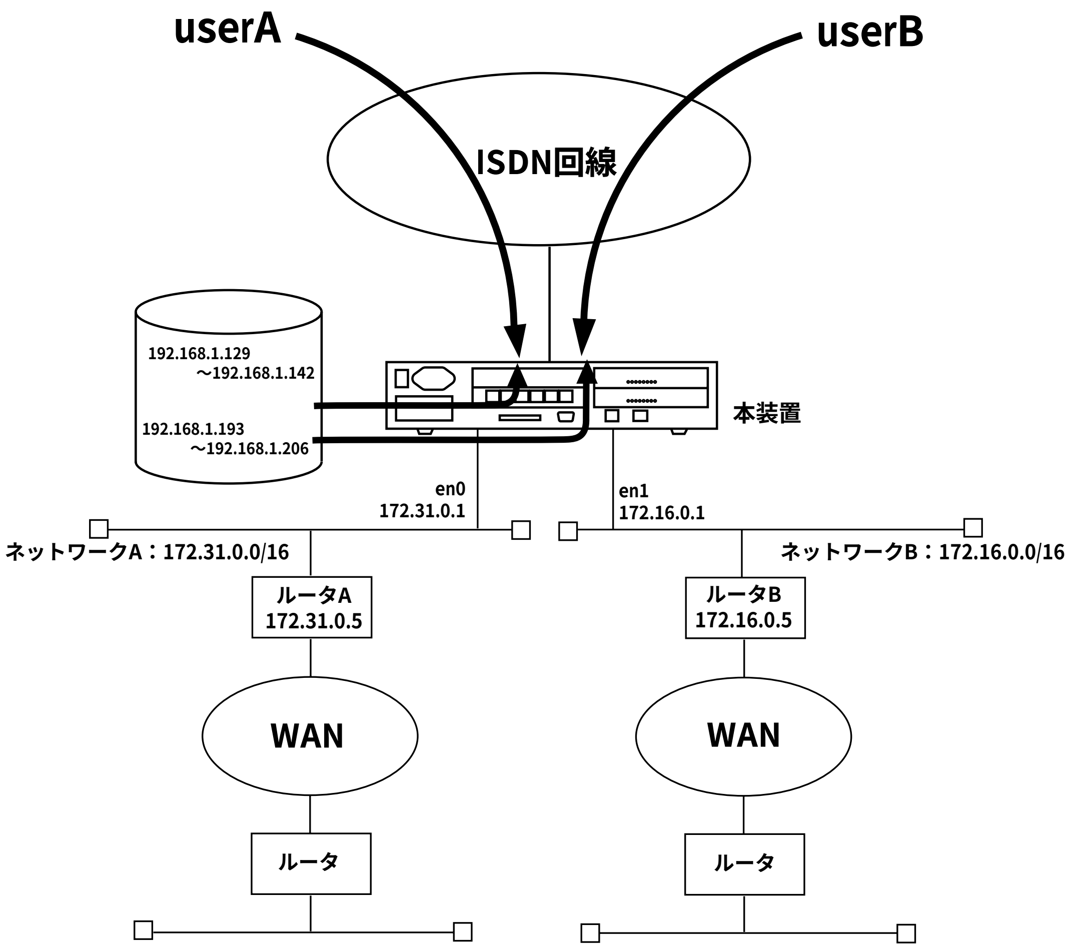
IPプールを使って接続相手にIPアドレスを割り当てる場合に、そのルートをRIPで広告する設定について説明します。

ここでは、IPプールに、

　192.168.1.129～192.168.1.142

　192.168.1.193～192.168.1.206

の合計28個のIPアドレスをプールし、このプールから接続相手にIPアドレスを割り当てる場合の設定例について説明します。



［rip.confファイルの設定］

```
interface      en0①
interface      en1①
destination    192.168.1.128/28           2②
destination    192.168.1.192/28           2②
```

［解　説］

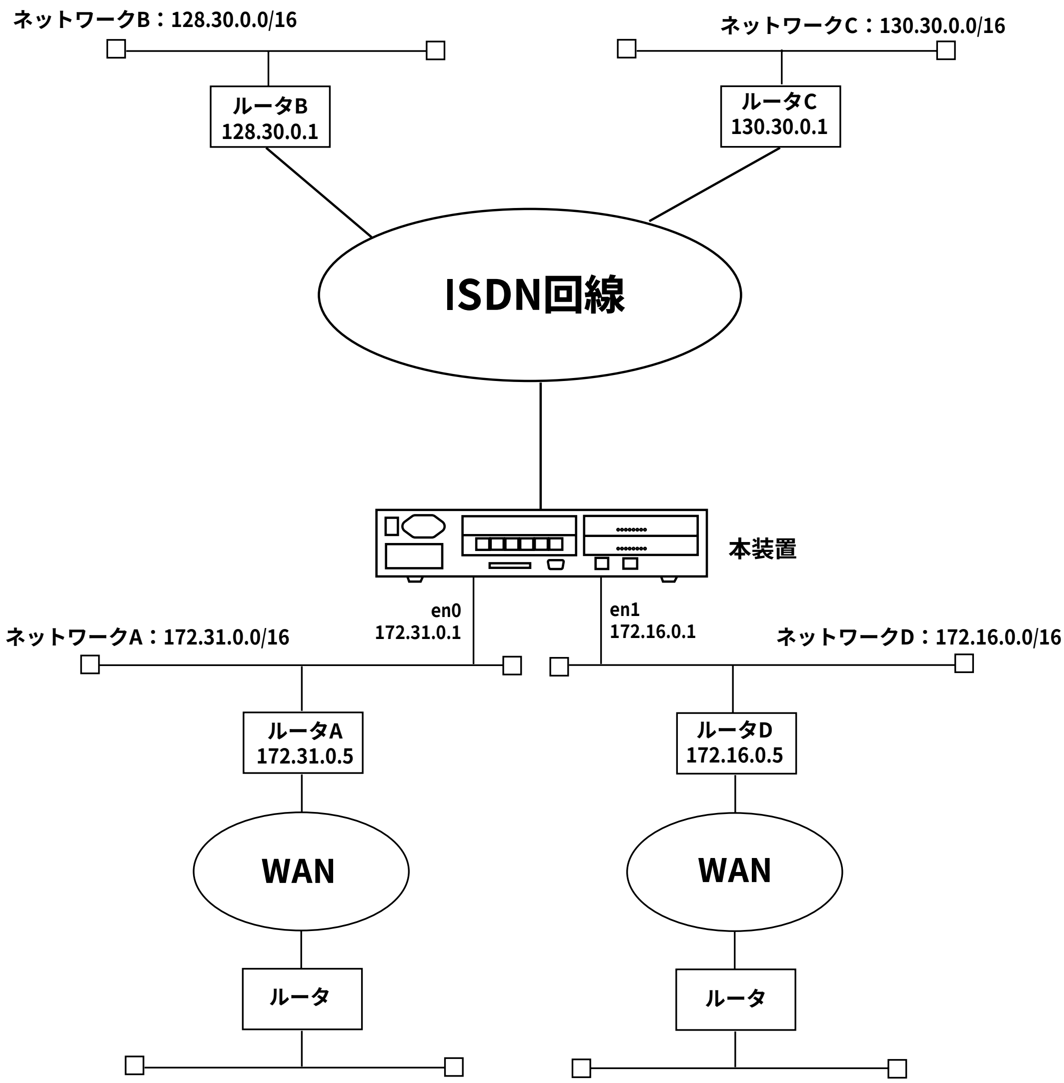
① en0、en1側はRIPを使って他のルータとルーティング情報を交換します。

② IPプールにプールされているIPアドレスを包含するようなルートをen0、en1に広告します。
送信の制御がRIP1の場合には、サブネットマスクを広告することができないので、宛先をネットワークアドレス(192.168.1.0/24)で広告します。
送信の制御がRIP2の場合には、サブネットマスクを広告することができるので、宛先をサブネットワークアドレス(192.168.1.128/28、192.168.1.192/28)で広告します。

IPプールを使用する場合の設定方法については、**「4.4.7　IPプールを使用する場合の設定」**を参照してください。

(2) ISDN側のルートを広告する場合の設定(ネットワーク型接続の場合)

ここでは、ISDN経由でネットワーク型接続を行う場合に、ISDN側のルートをRIPで広告する設定について説明します。



［rip.confファイルの設定］

```
interface     en0①
interface     en1①
destination   128.30.0.0/16  2②
destination   130.30.0.0/16  2②
```

［解　説］

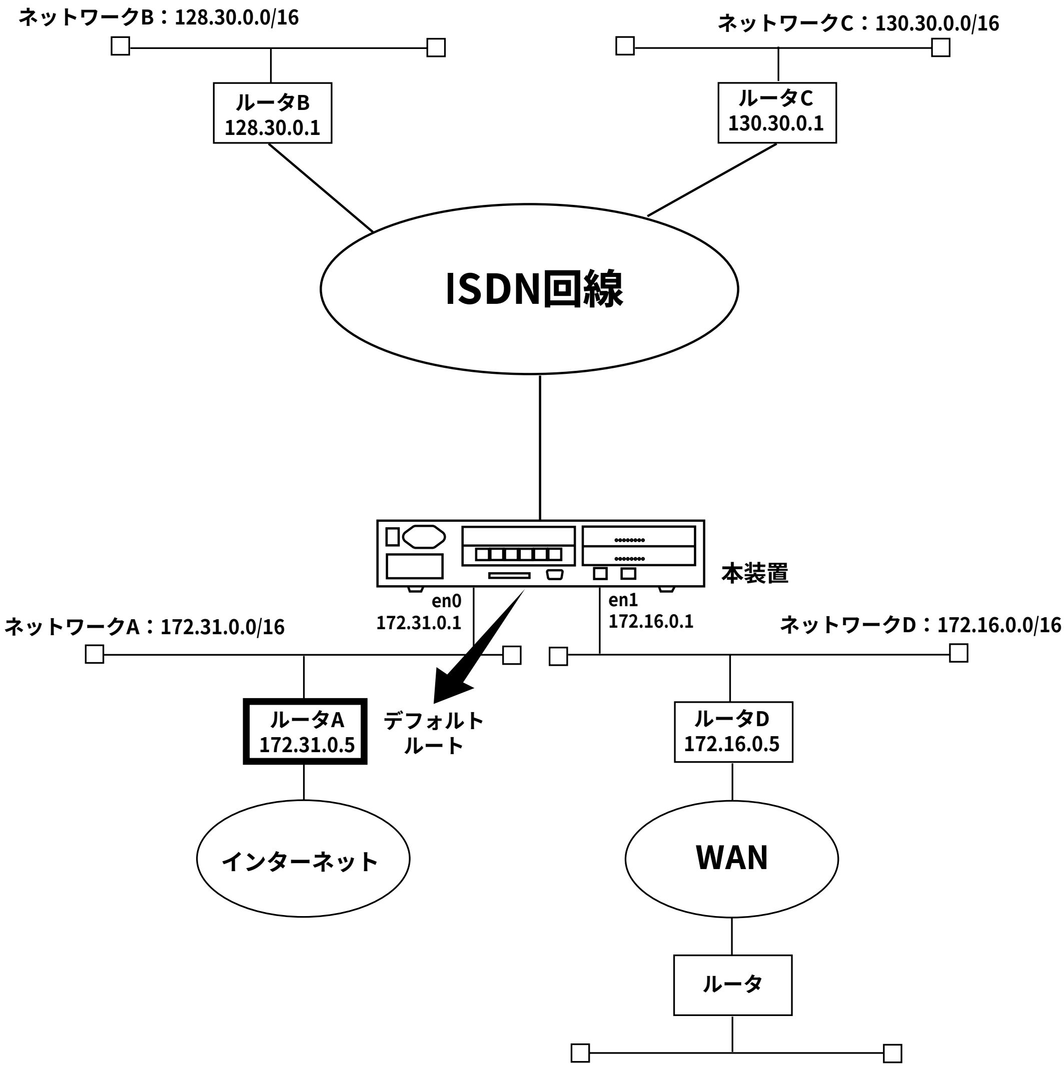
① en0、en1側はRIPを使って他のルータとルーティング情報を交換します。
② ISDN側のルート(128.30.0.0、130.30.0.0)をen0、en1にメトリック2で広告します。
送信の制御がRIP1の場合には、サブネットマスクを広告することができないので、宛先をネットワークアドレスで広告します。
送信の制御がRIP2の場合には、サブネットマスクを広告することができるので、宛先をサブネットワークアドレスで広告することができます。

ISDN側のルートはusersファイルに設定する必要があります。設定方法については、**「4.2 ISDN経由でネットワーク型接続を行う場合の基本的な設定」**を参照してください。

本装置はISDN側へルーティング情報を送信しません。そのため、ルータB、ルータCおよびネットワークB、ネットワークC上のホストにはスタティックにルーティング情報を設定する必要があります。

(3) デフォルトルートを広告する場合の設定

インターネットに接続しているルータがRIPの機能がなかったり、RIPの機能を停止させているなどのため、デフォルトルートを広告しない場合には、本装置がデフォルトルートを広告するようにできます。
ここでは、デフォルトルートの経由ルータがルータAの場合の設定例について説明します。



[rip.confファイルの設定]

```
interface     en0①
interface     en1①
destination   128.30.0.0/16  2②
destination   130.30.0.0/16  2②
destination   0.0/0  via    172.31.0.5    10③
```

[gatewaysファイルの設定]

```
destination   0.0/0  via    172.31.0.5    10④
```

［解　説］

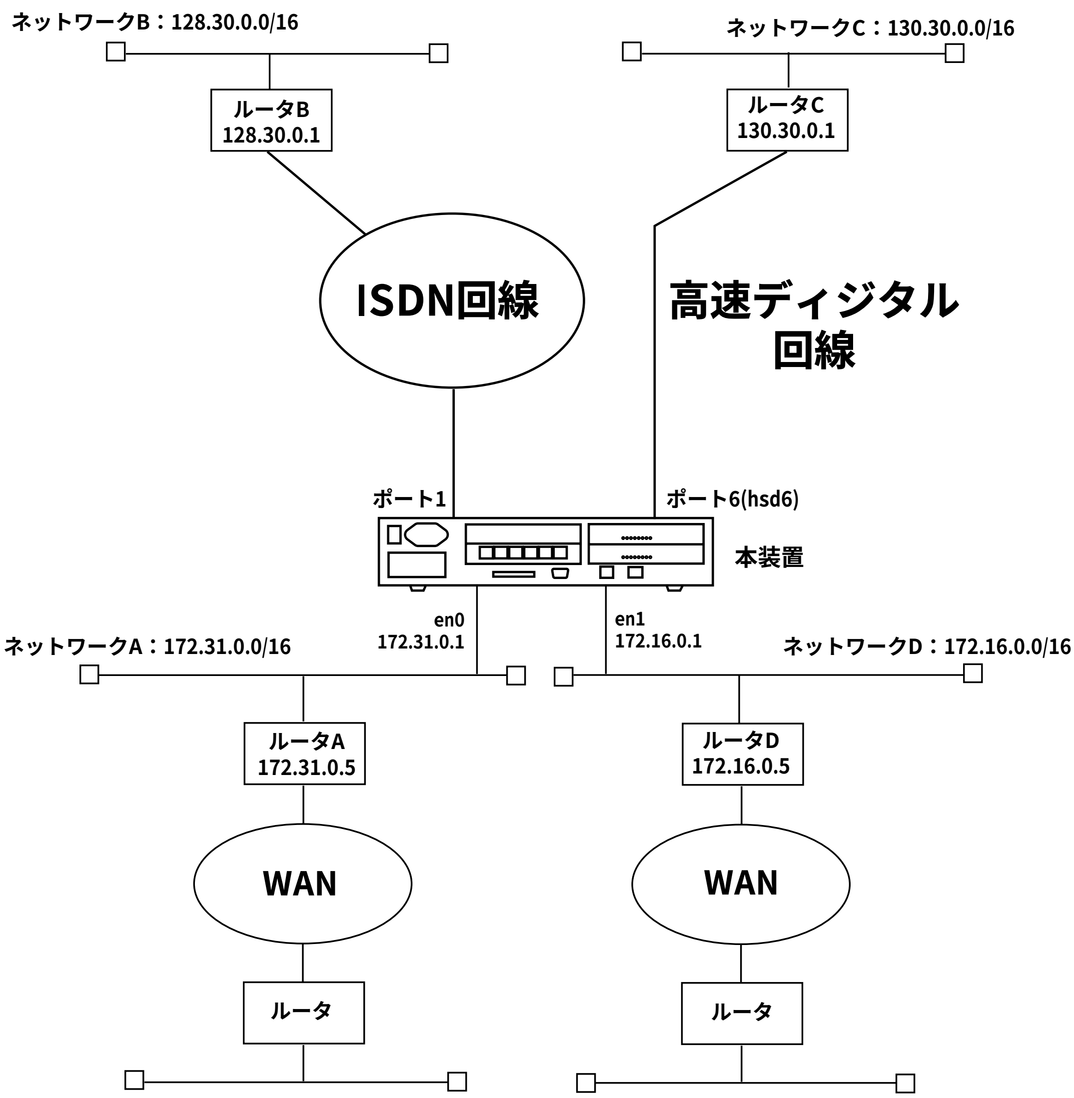
① en0、en1側はRIPを使って他のルータとルーティング情報を交換します。
② ISDN側のルート(128.30.0.0、130.30.0.0)をメトリック2でen0、en1に広告します。
送信の制御がRIP1の場合には、サブネットマスクを広告することができないので、宛先をネットワークアドレスで広告します。
送信の制御がRIP2の場合には、サブネットマスクを広告することができるので、宛先をサブネットワークアドレスで広告することができます。
③ デフォルトルートをルータAの代わりに広告します。経由ルータをルータA(172.31.0.5)に設定します。
④ 本当のデフォルトルートに関しては、gatewaysファイルに設定します。

ISDN側のルートはusersファイルに設定する必要があります。設定方法については、**「4.2 ISDN経由でネットワーク接続を行う場合の基本的な設定」**を参照してください。

本装置はISDN側へルーティング情報を送信しません。そのため、ルータB、ルータCおよびネットワークB、ネットワークC上のホストにはスタティックにルーティング情報を設定する必要があります。

(4) 高速ディジタル回線を使用してルートを広告する場合の設定

ここでは、ISDN側をネットワーク型接続で高速ディジタル回線インタフェースにはIPアドレスを設定しない場合を想定し、ISDN側のルートをRIPで広告する設定について説明します。



[rip.confファイルの設定]

```
interface     en0①
interface     en1①
interface     hsd6①
destination   128.30.0.0/16  2②
```

[解　説]

① en0、en1側およびhsd6側はRIPを使って他のルータとルーティング情報を交換します。
② ISDN側のルート(128.30.0.0)をメトリック2でen0、en1、hsd6に広告します。
送信の制御がRIP1の場合には、サブネットマスクを広告することができないので、宛先をネットワークアドレスで広告します。
送信の制御がRIP2の場合には、サブネットマスクを広告することができるので、宛先をサブネットワークアドレスで広告することができます。

ISDN側のルートはusersファイルに設定する必要があります。設定方法については、**「4.2 ISDN経由でネットワーク型接続を行う場合の基本的な設定」**を参照してください。
また、高速ディジタル回線側のルートは、ルータCとルーティング情報の交換を行うことによって自動的にルーティングテーブルを作成するため、gatewaysファイルにルーティング情報を設定する必要はありません。ただし、ルータCにRIPの機能がない場合や高速ティジタル回線上でRIPを使用しない場合には、高速ディジタル回線側のルートをgatewaysファイルに設定してください。設定方法については、**「4.3　高速ディジタル回線経由でネットワーク型接続を行う場合の基本的な設定」**を参照してください。

本装置はISDN側へルーティング情報は送信しません。そのため、ルータBおよびネットワークB上のホストにはスタティックにルーティング情報を設定する必要があります。

5章

セットアップファイル・リファレンス

5章では、本装置の動作を設定するための各セットアップファイルの記述方法について説明しています。
セットアップファイルの編集方法については**3章**、またシステム構成に応じた設定方法については**4章**で説明していますので、あわせてお読みください。

本章の内容

本装置では、各機能ごとに分かれたセットアップファイルを編集することによって、動作を指定します。
本装置で使用するセットアップファイルの一覧を、**表5-1**に示します。

表5-1　セットアップファイル一覧

ファイル名	設定内容
hostname	本装置のホスト名を設定します。
hosts	IPアドレスと対応するホスト名を設定します。
boards	拡張ボードの使用方法を設定します。
interface	ネットワークインタフェースの設定をします。
gateways	スタティックルーティングの設定をします。
ipfilters	IPフィルタを設定します。
netmask	サブネットマスクを設定します。
resolv.conf	DNSのリゾルバを設定します。
snmpconf	SNMPの情報を設定します。
users	ISDN経由で接続する接続相手の設定を行います。
radius	RADIUSサーバとの通信に関する設定を行います。
ippool	IPプール機能を使用する場合に、プールするIPアドレスを設定します。
servers	ブート時に起動させる各種サーバプログラムを設定します。
rip.conf	RIPの設定を行います。
syslog.conf	syslogの設定を行います。
services	サービス名とポート番号の対応を設定します。

本章で使用される主な設定項目の書式を説明します。

<名前>	：	このフィールドの名称を示すもので、実際のセットアップファイルには、このフィールドに使用できる値を設定します。
[A]	：	[ ]内のフィールドが省略可能であることを示します。
{A｜B}	：	{ }内のいずれかのフィールドを選択することを示します。
A．．．	：	Aと同様の項目が列挙できることを示します。

<ホスト名>

ネットワーク上のノードのホスト名を、半角の英数字（最大63文字）で指定します。

<IPアドレス>

IPアドレスをドットで区切られた0〜255の10進数で指定します。

例： **10.0.0.1**
172.16.1.32

<マスク>

IPアドレスに対するマスクビットを指定します。マスクビットの指定方法には、以下のものがあります。

マスクビット長	：１から32の10進数でビット長を指定します。 例：24
マスクパターン	：ドットで区切られた0〜255の10進数でマスクパターンを指定します。
host	：ホストに対するマスクを意味します。
net	：IPアドレスのクラスに対応したマスクを意味します。
subnet	：netmaskファイルに設定したサブネットマスクに対応したマスクを意味します。

<論理インタフェース>

本装置で決められている論理インタフェース名を半角の英数字で指定します。

論理インタフェース名	説　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
isdn0	ISDN回線の論理インタフェース名
hsd＊	高速ディジタル回線の論理インタフェース名 「hsd＊」はinterfaceファイルのinterfaceキーワードで設定した論理インタフェース名です。 （＊：1〜）
ncp＊	ISDN回線の場合に本装置内部で使用する論理インタフェース名 「ncp＊」は発着信時に本装置が自動的に選択する論理インタフェース名で、どの接続相手がどの論理インタフェースを使用するかについては、その時の状態に応じて変化します。 （＊：0〜）
P1-＊PRI	SNMPのリンクUP / DOWNトラップで使用する論理インタフェース名 「P1-＊PRI」は拡張ボードスロット番号1とPRIポート番号の論理インタフェース名です。 ＊：PRIポート番号（1〜6）
lo0	本装置内部で使用するループバック用の論理インタフェース名 特にセットアップやコマンド等で使用することはありません。
sink0	本装置内部で使用するnoforward用の論理インタフェース名 特にセットアップやコマンド等で使用することはありません。
ipnhr0	本装置内部で使用するフォワーディング用の論理インタフェース名 特にセットアップやコマンド等で使用することはありません。

5.1 hostnameファイル

本装置のホスト名を設定します。

書　式　　**<ホスト名>**

例　　**ns4200**

解　説　　本装置のホスト名を指定します。指定したホスト名は、hostsファイルにも登録する必要があります。

注　意　　**hostnameファイルの変更を有効にするには、リブートが必要です。**

5.2　hostsファイル

ネットワーク上のホスト名と、対応するIPアドレスを設定します。

書　式　　**<IPアドレス>　<ホスト名>　[<ホスト別名>]**

例　　**172.31.2.1 ns4200 routerA**

解　説　　ネットワーク上のホストコンピュータやルータのホスト名と、それに対応するIPアドレスを指定します。そのノードがホスト別名を持っている場合には、その名前を**<ホスト別名>**に設定します。

注　意　　**本装置のホスト名（hostnameファイルに設定したホスト名）に対応するIPアドレスは必ず設定してください。また、本装置のhostnameに対応するIPアドレスを変更する場合には、本装置のリブートが必要です。**

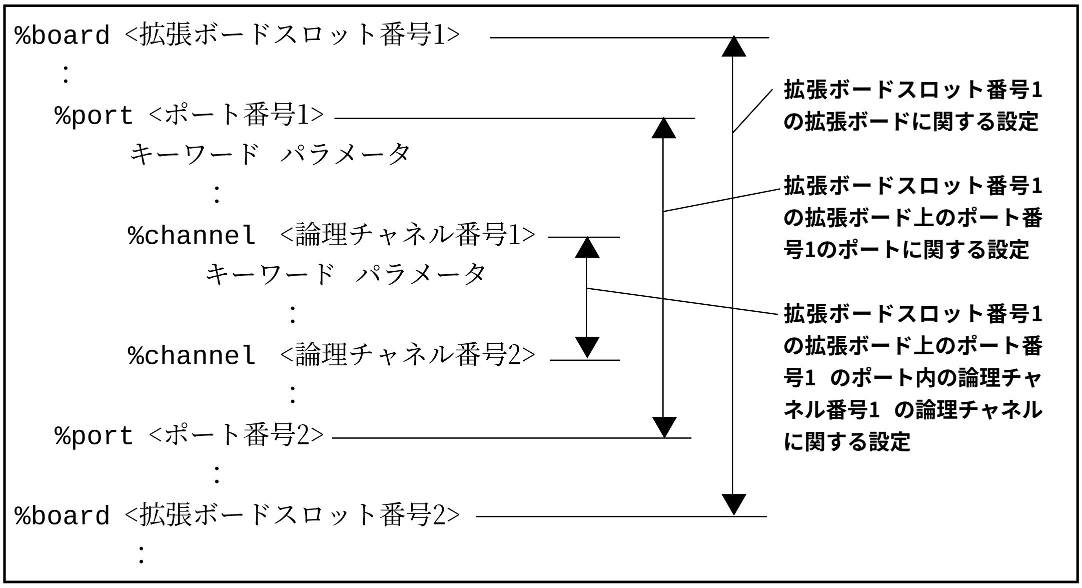
注　意　　**hostsファイルの変更は、アプリケーションがこのファイルを参照する時点で有効になります。すなわち、telnetクライアントなどは、telnetコマンド実行時にhostsファイルの変更が有効になります。また、他のセットアップファイルからホスト名を参照している場合には、そのセットアップファイルが有効となる時点（例えば、reloadコマンド実行時）にhostsファイルの変更が有効になります。**

注　意　　**hostsファイルには、工場出荷時に以下の2つのIPアドレスが設定されています。これらは、本装置の内部で使用していますので削除しないでください。**

127.1　　localhost　loghost
127.2　　noforward

5.3 boardsファイル

NS-420 PRI拡張ボードに関して、その使用方法を設定します。
本セットアップファイルは、階層的に拡張ボードスロットに挿入されている拡張ボードの設定から、物理ポートの設定、論理チャネルの設定と行います。
本セットアップファイルの全体の構成は、以下のようになっています。



まず、%board分類キーワードで、設定する拡張ボードが挿入されている拡張ボードスロット番号を指定します。次に、%port分類キーワードで、その拡張ボードのポート番号を指定し、続いてポートに関する設定を行います。必要に応じて%channel分類キーワードで論理チャネル番号の指定と、論理チャネルに関する設定を行います。

boardsファイルで使用する分類キーワードの一覧を**表5-2**に示します。

表5-2 boardsファイルの分類キーワード一覧

分類キーワード	説　明
%board	拡張ボードの設定をする。
%port	拡張ボード上の物理ポートの設定をする。
%channel	物理ポート上の論理チャネルの設定をする。

%board

分類キーワード **boardsファイル**

書　式　**%board　<拡張ボードスロット番号>**

設定範囲　**1～4**

例　**%board 1**

解　説　拡張ボードが挿入されている拡張ボードスロット番号を指定します。
次の「%board」が現れるか、boardsファイルが終わりになるまでの間の分類キーワードやキーワードで設定した内容が、その拡張ボードの情報になります。

注　意　**当面、拡張ボードスロット番号は1のみです。**

%port

分類キーワード **boardsファイル**

書　式　**%port　<ポート番号>**

設定範囲　**1～6**

例　**%port 6**

解　説　拡張ボード上の物理ポート番号を指定します。
次に「%port」、「%board」が現れるまで、または、boardsファイルが終わりになるまでの間の分類キーワードやキーワードで設定した内容が、その物理ポートの情報になります。

line_type

キーワード **boardsファイル**

書　式　**line_type　<回線種別>**

設定値　**isdn / hsd**

例　**line_type isdn**

解　説　指定したポートの回線種別を設定します。

- isdn　：指定したポートをISDN回線として使用します。指定のポートにISDN回線を接続してください。
- hsd　：指定したポートを高速ディジタル回線として使用します。指定のポートに高速ディジタル回線を接続してください。

telnumber

キーワード **boardsファイル**

書　式　**telnumber　<電話番号>[*<サブアドレス>]**

例　1　**telnumber 043-222-3333**

例　2　**telnumber 01-2345-6789*abc**

解　説　指定したポートに自局電話番号および自局サブアドレスを設定します。
自局サブアドレスを設定する場合、あるいは代表取扱サービスを使用している場合に代表番号以外の契約番号を相手に通知したい場合などには、ISDNポートの自局電話番号を設定します。通常は設定する必要はありません。
<電話番号>には、区切り記号として「-」(ハイフン)を使用できます。
<サブアドレス>を指定する場合には、例2のように電話番号の後ろに「*」を付けて、その後ろにサブアドレスを記述します。サブアドレスは、英数字で最大19文字です。

注　意　**本キーワードは、ISDN回線(line_type isdn)の場合のみ有効です。**

enable / disable

キーワード **boardsファイル**

書　式　**enable**
書　式　**disable**

デフォルト　**enable**

解　説　**「enable」の場合、そのポートが使用可能になります。「disable」に設定すると、そのポートは使用禁止となります。**

関　連　**wanportコマンド**

参　照　**「6章　wanportコマンド」**

clid_require

キーワード **boardsファイル**

書　式　**clid_require　{on｜off}**

デフォルト　**off**

解　説　発信者番号通知のない着信を拒否するかどうかを設定します。
on ：発信者番号通知のない着信を拒否する。
off ：発信者番号通知のない着信を拒否しない。

注　意　**本キーワードは、ISDN回線(line_type isdn)の場合のみ有効です。**

%channel

分類キーワード **boardsファイル**

書　式　**%channel　<論理チャネル番号>**

設定範囲　**1～24**

例　**%channel 1**

解　説　ポート内の論理チャネル番号を指定します。
次に「%channel」、「%port」、「%board」が現れるまで、または、boardsファイルが終わりになるまでの間のキーワードで設定した内容が、その論理チャネルの情報になります。

注　意　**本分類キーワードは、高速ディジタル回線(line_type hsd)の場合のみ有効です。**

slots

キーワード **boardsファイル**

書　式　　**slots　<タイムスロット番号>**

設定範囲　　**1〜24**

例　１　　**slots 1**

例　２　　**slots 1,5**

例　３　　**slots 1-24**

解　説　　指定した論理チャネルが使用するタイムスロットの範囲を設定します。範囲の記述方式としては、カンマ「,」とハイフン「-」が使用でき、カンマはアンドを意味し、ハイフンは範囲(レンジ)を意味します。例1はタイムスロット1を、例2はタイムスロット1と5を、例3はタイムスロット1から24までを、それぞれ使用して通信することを示しています。

注　意　　**本キーワードは、高速ディジタル回線(line_type hsd)の場合のみ有効です。**

5.4 interfaceファイル

IPで使用するネットワークの論理インタフェースに関して設定します。

注　意　**ISDNの論理インタフェースは、usersファイルに設定しますのでinterfaceファイルに設定する必要はありません。**

interface

キーワード　**interfaceファイル**

書　式　**interface　<論理インタフェース名>[/<自局IPアドレス>] <相手IPアドレス>[/<マスク>]　<属性>**

例　1　**interface en0 */* numbered**
例　2　**interface en0/172.31.0.1 172.31.0.0/24 numbered**
例　3　**interface en0/172.31.0.1 172.31.0.0/24 numbered,down**
例　4　**interface hsd1 172.31.0.1 unnumbered**

解　説　interfaceファイルには、IPで使用する論理インタフェースに関する設定をします。ただし、ISDNの論理インタフェース（isdn0）はusersファイルに設定します。各論理インタフェースをinterfaceキーワードで区切って指定します。オプションとして、サブキーワードによりIPフィルタに関する設定ができます。

<論理インタフェース名>　論理インタフェース名を指定します。

論理インタフェース名	説　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
hsd∗	高速ディジタル回線の論理インタフェース名（∗：1～）

<自局IPアドレス>　論理インタフェースに固有の自局IPアドレスを割り当てる場合には、対応する自局のIPアドレスを設定します。
例１のように、論理インタフェースen0に自局IPアドレスを省略した場合には、本装置のホスト名に対応するIPアドレスが割り当てられます。
また、例４のように、論理インタフェースhsd1に自局IPアドレスを割り当てない設定ができます。

<相手IPアドレス>　この論理インタフェースに直接接続されている相手ルータのIPアドレスまたはネットワークのアドレスを設定します。
例１のように**<相手IPアドレス>/<マスク>**に「*/*」を設定した場合は、本装置のホスト名に対応するIPアドレスのネットワークアドレスが設定されます。例えば、本装置のホスト名に対応するIPアドレスが172.16.2.2ならば、172.16.0.0/16の設定と同等です。

<マスク>　相手IPアドレスのマスクを設定します。

<属性>　論理インタフェース固有のIPアドレスを割り当てる場合には、numberedを設定します。イーサネットのようなネットワークインタフェースには、numberedの設定をします。
固有のIPアドレスを割り当てない場合には、unnumberedを指定します。
この論理インタフェースをダウンにする場合には、カンマ「,」に続けてdownと設定します。

inferfaceキーワードでは、次の行からサブキーワードを記述できます。

filter

サブキーワード　　**interfaceファイル**

書　式　　**filter　<フィルタ名>**

例　　**filter telFIL**

解　説　　この論理インタフェースに直結したセグメント宛のパケットに対するフィルタ条件を設定します。指定したフィルタ条件に一致したパケットのみが、このセグメントにフォワーディングされます。

<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

注　意　　**フィルタが適用されるのは、この論理インタフェースに直結したセグメント宛のパケットです。この論理インタフェースを経由して接続された先のセグメント当てのフィルタを指定する場合には、gatewaysファイルに設定してください。**

access

サブキーワード **interfaceファイル**

書　式　**access　{include｜exclude}　<フィルタ名>**

例　1　**access include ftpFIL**
例　2　**access exclude telFIL**

解　説　この論理インタフェースの入力フィルタ条件を設定します。指定したフィルタ条件に一致したパケットのみを通過させたり、反対にフィルタに一致したパケットを廃棄することができます。入力フィルタの処理はパケットの受信処理で行われますので、ここで廃棄されたパケットはフォワーディングされることはありません。
また、本装置宛てのパケットもフィルタすることができますので、本装置への不正アクセスを防止する効果もあります。
includeは、フィルタに一致したパケットのみを通過させる場合に指定します。
excludeは、フィルタに一致したパケットを廃棄させる場合に指定します。
includeとexcludeの両方とも指定した場合には、includeのフィルタに一致せず、かつexcludeのフィルタに一致したパケットのみが廃棄され、それ以外のパケットはすべて通過します。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

outputfil

サブキーワード **interfaceファイル**

書　式　**outputfil　<フィルタ名>**

例　**outputfil telFIL**

解　説　この論理インタフェースに出力フィルタをかけたい場合、その条件を設定します。指定したフィルタ条件に一致したパケットのみが出力されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

phy

サブキーワード **interfaceファイル**

書　式　**phy　{{10｜100}　[full]}**

例　1　**phy 10**

例　2　**phy 100 full**

解　説　phyは、論理インタフェースen0、en1についてのみ有効です。
通常は、このサブキーワードを指定する必要はありません。
phyサブキーワードを省略した場合、LANポートを100M／10Mの自動切り替えで使用します。
LANポートを固定で使用したい場合にのみ、phyサブキーワードで以下の値を指定してください。

10	：	10M固定
100	：	100M固定
full	：	fullデュプレックス固定

broadcast

サブキーワード **interfaceファイル**

書　式　**broadcast　<IPアドレス>　[default]**

例　**broadcast 128.30.0.0**
broadcast 128.30.255.255 default

解　説　通常は、このサブキーワードを指定する必要はありません。
broadcastサブキーワードを省略した場合は、ブロードキャストアドレスとして「255.255.255.255」が使用されます。これ以外のブロードキャストアドレスを使用しているホストがある場合のみ設定が必要です。
本装置がブロードキャストアドレスとして受信／送信するアドレスを設定します。複数のブロードキャストアドレスを指定することができます。

<IPアドレス>　ブロードキャストアドレスを指定します。
[default]　このアドレスが本装置が送信するパケットのブロードキャストアドレスとして使用されます。「default」を指定できるのは、1つだけです。

proxyarp

サブキーワード **interfaceファイル**

書　式　**proxyarp　on_demand　{auto｜all｜off}**

デフォルト　**auto**

例　**proxyarp on_demand all**

解　説

proxyarpサブキーワードは、PPPのアドレスネゴシエーションにおいて割り当てた相手IPアドレスを、この論理インタフェースでProxy ARPで応答するかどうかの設定を行います。
autoは、割り当てた相手IPアドレスが、この論理インタフェースと同じネットワークに属するアドレスの場合に、Proxy ARPで応答するように設定します。
allは、割り当てた相手IPアドレス全てをProxy ARPで応答するように設定します。
offは、割り当てた相手IPアドレスをproxy ARPで応答するようには設定しません。

注　意

proxyarpサブキーワードは、LANの論理インタフェースen0、en1でのみ有効です。

channel

サブキーワード **interfaceファイル**

書　式　**channel　<拡張ボードスロット番号>/<ポート番号>/<論理チャネル番号>**

例　**channel 1/2/1**

解　説

高速ディジタル回線を使用する場合に、この論理インタフェースに論理チャネルを対応させます。
<拡張ボードスロット番号>、**<ポート番号>**と**<論理チャネル番号>**は、それぞれboardsファイルで設定した拡張ボードスロット番号(%board分類キーワード)、ポート番号(%port分類キーワード)と論理チャネル番号(%channel分類キーワード)に対応しています。

5.5　gatewaysファイル

ディスティネーションごとのスタティックルーティング情報を設定します。

destination

キーワード　　**gatewaysファイル**

書　式　**destination　<宛先アドレス>[/<マスク>]　via　<経由ルータ>　<メトリック>**

例　**destination 128.30.0.0/net via 128.30.0.2 2**
destination 128.30.0.1/host via 128.30.0.3 2

解　説　gatewaysファイルにはスタティックなルーティング情報を設定します。各デスティネーションについて、経由するルータとメトリックを指定します。
フォワーディングされるパケットの宛先IPアドレスがgatewaysファイルに設定した**<宛先アドレス>/<マスク>**と比較され、一致した経路の**<経由ルータ>**にフォワーディングされます。もし、複数の経路と一致した場合には、最もマスク長の長い経路にフォワーディングされます。

<宛先アドレス>　デスティネーションのネットワークアドレス、またはホストアドレスを設定します。例１の設定において、128.30.0.0のネットワーク宛てのパケットは128.30.0.2のルータに送られますが、128.30.0.1宛てのパケットは128.30.0.3のルータに送られます。

<マスク>　**<宛先アドレス>**に対するマスクを設定します。フォワーディングされるパケットの宛先IPアドレスに、このマスクをかけた結果と**<宛先アドレス>**が比較されます。

<経由ルータ>　パケットをフォワーディングするルータの<IPアドレス>または<ホスト名>を指定します。
特別な経由ルータとして、廃棄したいパケットをフォワーディングするための仮想ルータnoforwardがあります。（詳細はnoforwardフィールドキーワード参照）

<メトリック>　この経路のメトリックを10進数で設定します。範囲は1から99です。フォワーディングされるパケットが複数の経路に一致し、最大のマスク長となる経路が複数存在する場合には、このメトリックが小さい方の経路が選択されます。

デフォルトルートを設定する場合には、次のように宛先アドレス／マスクを「0.0/0」と設定してください。

デフォルトルートの設定例

```
destination   0.0/0   via   128.30.0.4   2
```

noforward

フィールドキーワード **gatewaysファイル**

書　式　**destination　<宛先アドレス>[/<マスク>]　via　noforward　<メトリック>**

例

destination 172.16.1.0/24 via 128.30.0.2 2
destination 172.16.1.0/24 via noforward 1
filter telFIL

解　説

noforwardは、廃棄したいパケットをフォワーディングするための**<経由ルータ>**で、予めhostsファイルに登録されているホスト名です。ルーティング選別用のIPフィルタ(filterサブキーワードで指定)では一致したパケットを通過させることはできますが一致したパケットを廃棄することはできません。そこで、フィルタに一致したパケットを廃棄するには、この仮想ルータnoforwardを指定してパケットを廃棄します。

例では、172.16.1.0のネットワーク宛てのパケットの内、フィルタ名 telFILに一致したパケットは仮想ルータnoforwardに送られ廃棄されます。

filter

サブキーワード **gatewaysファイル**

書　式　**filter　<フィルタ名>**

例　**filter telFIL**

解　説

このデスティネーション宛のパケットに対するフィルタ条件を設定します。指定したフィルタ条件に一致したパケットのみが、このデスティネーションにフォワーディングされます。

<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

5.6 ipfiltersファイル

パケットフィルタを定義するファイルです。
ipfiltersで定義したフィルタは、interfaceファイル、gatewaysファイル、usersファイル、および radiusファイルで参照して使用します。

注　意　**IPフィルタ（gatewaysファイル、interfaceファイル、およびusersファイルのfilterキーワードで指定したもの、およびradiusファイルのdefault_filterキーワードで指定したもの）やアウトプットフィルタ（interfaceファイル、およびusersファイルのoutputfilキーワードで指定したもの、およびradiusファイルのdefault_outputfilキーワードで指定したもの）は、フォワーディングに関してのみ有効です。すなわち、本装置自身の送信パケットには影響しません。**

注　意　**IPオプションを含むIPパケットでは、IPフィルタは無視されてルーティングされます。また、アウトプットフィルタも無視されて出力されます。**

注　意　**IPパケットがフラグメンテーションされている場合には、1番目のフラグメント情報に従ってフィルタリングされます。ただし、一定時間以上経過してから2番目以降のフラグメントを受信した場合には、このフラグメント情報は失われますので、IPフィルタは無視されてルーティングされます。また、アウトプットフィルタも無視されて出力されます。**

%FILTER

分類キーワード　　**ipfiltersファイル**

書　式　**%FILTER　<フィルタ名>**
<フィルタ本体>

例

```
%FILTER telnetFIL
          PROTO=ICMP
OR        PROTO=TCP AND SPORT=telnet
OR        PROTO=TCP AND DPORT=telnet
```

解　説　フィルタの名称を定義します。
%FILTERの次の行から、このフィルタの本体を定義します。フィルタ本体は次の分類キーワードまたはファイルの終わりまで続きます。
フィルタ本体はフィルタエントリをORで結合したもので構成されます。
各フィルタエントリは、フィールドエントリをANDで結合したもので構成されます。
OR演算子よりもAND演算子の方が優先されます。
フィールドエントリを定義するための、予約語の一覧および演算子の一覧を次に示します。
予約語は、すべて大文字または小文字で記述してください。

表5-3　IPフィルタのフィールド名称

フィールド名称	意　味
SA (sa)	発信元IPアドレス
DA (da)	宛先IPアドレス
PROTO (proto)	上位層プロトコル識別子
TOS (tos)	サービス種別
SPORT (sport)	発信元ポート番号
DPORT (dport)	宛先ポート番号
INTERFACE (interface)	そのパケットが受信されたインタフェース名

表5-4　演算子一覧

演算子	意　味	使用可能な項目
=	一致	発信元IPアドレス、宛先IPアドレス、プロトコル、発信元ポート番号、宛先ポート番号、TOS、入力インタフェース
!=	不一致	発信元IPアドレス、宛先IPアドレス、プロトコル、発信元ポート番号、宛先ポート番号、TOS、入力インタフェース
<	より小さい	発信元ポート番号、宛先ポート番号
>	より大きい	発信元ポート番号、宛先ポート番号

%CONST

分類キーワード　　　　**ipfiltersファイル**

書　式　　**%CONST**

　　<定義名称>=<値>

例　　**%CONST**

　　ICMP=1

　　TCP=6

　　UDP=17

解　説　　ipfiltersファイル内で使用する定数を定義します。
%CONSTの次の行から、定数を定義します。定数の定義は次に分類キーワードが現れるかファイルの終わりまで続きます。

注　意　　**定数の定義は、ファイル内でこの定数が参照される以前に定義されている必要があります。**

SA

フィールドキーワード **ipfiltersファイル**

書　式　**SA　<演算子>　<IPアドレス>[/<マスク>]**

例
SA = 172.16.31.1
SA = 172.17.1.0/24
SA = yuka
SA != 10.0.0.0/8

解　説　発信元IPアドレスを指定します。ホストアドレスをドット記法またはhostsファイルに登録したホスト名で指定できます。また、マスクを指定してネットワークアドレスを指定できます。
<演算子>　「=」と「!=」が使用可能です。

DA

フィールドキーワード **ipfiltersファイル**

書　式　**DA　<演算子>　<IPアドレス>[/<マスク>]**

例
DA = 172.16.31.1
DA = 172.17.1.0/24
DA = yuka
DA != 10.0.0.0/8

解　説　宛先IPアドレスを指定します。ホストアドレスをドット記法またはhostsファイルに登録したホスト名で指定できます。また、マスクを指定してネットワークアドレスを指定できます。
<演算子>　「=」と「!=」が使用可能です。

PROTO

フィールドキーワード **ipfiltersファイル**

書　式　**PROTO　<演算子>　<番号>**

例
PROTO = 17
PROTO = TCP
PROTO != UDP

解　説　IPの上位層プロトコル識別子の番号を10進数で指定します。例のように、%CONSTで定義した名称（TCP）を指定することもできます。
<演算子>　「=」と「!=」が使用可能です。

TOS

フィールドキーワード **ipfiltersファイル**

書　式　**TOS　<演算子>　<番号>**

例　**TOS = 1**
TOS != 1

解　説　IPのサービス種別（Type Of Service）の番号を指定します。
<演算子>　「=」と「!=」が使用可能です。

SPORT

フィールドキーワード **ipfiltersファイル**

書　式　**SPORT　<演算子>　<番号>**

例　**SPORT = 23**
SPORT = telnet
SPORT != 21
SPORT < 1024
SPORT > 128

解　説　IPの発信元ポート番号の値を10進数で指定します。また、値としてservicesファイルに登録されているサービス名を使用することもできます。
<演算子>　「=」,「 !=」,「<」,「>」が使用可能です。

注　意　**上位層プロトコルがTCPまたはUDP以外の場合には、このフィールドキーワードは指定しないでください。**

DPORT

フィールドキーワード **ipfiltersファイル**

書　式　**DPORT　<演算子>　<番号>**

例

DPORT = 21
DPORT = ftp
DPORT != 23
DPORT < 1024
DPORT > 128

解　説　IPの宛先ポート番号の値を10進数で指定します。また、値としてservicesファイルに登録されているサービス名を使用することもできます。
<演算子>　「=」,「 !=」,「<」,「>」が使用可能です。

注　意　**上位層プロトコルがTCPまたはUDP以外の場合には、このフィールドキーワードは指定しないでください。**

INTERFACE

フィールドキーワード **ipfiltersファイル**

書　式　**INTERFACE　<演算子>　<論理インタフェース名>**

例

INTERFACE = en0
INTERFACE != en1

解　説　IPパケットを受信した論理インタフェースを指定します。
<演算子>　「=」と「!=」が使用可能です。

5.7　netmaskファイル

本装置を接続するネットワークがサブネットワークを使用している場合、IPのサブネットマスクを設定します。

書　式　　**<ネットワークアドレス>　<マスク値>**

例　　**123.30.0.0 255.255.255.0**

解　説　　**<ネットワークアドレス>**には、接続するネットワークアドレスを設定します。
<マスク値>は、8桁の16進数でも設定できます。

注　意　　**サブネットマスクの設定は、通常interfaceファイルを使用してください。netmaskファイルは旧製品との互換性を持つために残されているファイルです。**

5.8 resolv.confファイル

DNS（Domain Name System）を使用してネットワーク上のホスト名を管理している場合に、本装置が照会するネームサーバやデフォルトのドメイン名を設定します。

domain

キーワード **resolv.confファイル**

書　式　**domain　<ドメイン名>**

例　**domain sample.edu**

解　説　**<ドメイン名>**は、ホスト名の最後に「.」(ドット)がついていない場合に、ネームサーバに照会する際にホスト名の後に本装置が補填するドメイン名です。例えば、ホスト名に「seiko」を指定すると「seiko.sample.edu.」でネームサーバに照会されます。

nameserver

キーワード **resolv.confファイル**

書　式　**nameserver　<IPアドレス>**

例　**nameserver 128.30.0.3**

解　説　**<IPアドレス>**は、DNSで照会するネームサーバのIPアドレスです。ネームサーバは最大で3個まで設定できます。複数のネームサーバを登録した場合には、最初のネームサーバの照会がタイムアウトした場合に、次のネームサーバに照会します。

5.9　snmpconfファイル

SNMP（Simple Network Management Protocol）のエージェント機能に関する設定をします。アクセスを許可するコミュニティ名の設定や、トラップの送信先ホスト、トラップの条件などの設定ができます。

sysContact

キーワード　　**snmpconfファイル**

書　式　　**sysContact　<文字列>**

例　　**sysContact "Y.Watanabe 700-7777"**

解　説　　この装置の管理者の名前や所属、電話番号などの情報を文字列で設定します。文字列は「"」でくくって設定します。

sysLocation

キーワード　　**snmpconfファイル**

書　式　　**sysLocation　<文字列>**

例　　**sysLocation "Server Room 16F HQ Building in TOKYO"**

解　説　　この装置の設置場所の情報を文字列で設定します。文字列は「"」でくくって設定します。

trap

キーワード　　**snmpconfファイル**

書　式　　**trap　<送信先のホスト>　[<コミュニティ名>　[<送信元IPアドレス>]]**

例　　**trap 172.16.1.3 public**
trap managerA
trap managerB public 172.16.1.100

解　説　　SNMPトラップの送信先のホストおよびコミュニティ名と、トラップの送信元IPアドレスを設定します。
送信先のホストはIPアドレスまたはhostsファイルに設定したホスト名で指定できます。コミュニティ名を省略した場合には、コミュニティ名を含まないトラップが送信されます。

送信元IPアドレスを省略した場合には、本装置のホスト名に対応するIPアドレスが使用されます。

注　意
- **トラップの送信先は最大20個まで設定できます。**
- **送信元のIPアドレスは、interfaceファイルなどで、本装置のIPアドレスとして、あらかじめ設定されている必要があります。**

community

キーワード　　**snmpconfファイル**

書　式　**community　<コミュニティ名>　{view1｜view2}　[<マネージャのIPアドレス>　・・・]**

例　1　**community *　view1**
例　2　**community admin view2**
例　3　**community admin view2 172.16.1.1**

解　説　アクセスを許可するコミュニティ名と、そのビューを設定します。
<コミュニティ名>にはそのコミュニティ名か「*」を設定します。「*」は、すべてのコミュニティ名を意味します。
ビューは、リードのみ許可する場合には「view1」を指定します。リード／ライトの両方を許可する場合には、「view2」を指定します。
例1では、すべてのコミュニティからのリードを許可し、例2ではコミュニティadminからのリード／ライトのアクセスを許可しています。
また、アクセスを認めるSNMPマネージャのIPアドレスを指定することができます。マネージャのIPアドレスは、IPアドレスまたはマネージャのIPアドレスを指定すると、そのIPアドレスのマネージャ以外からはアクセスできなくなります。例2を例3のようにすると、コミュニティ名がadminで、かつIPアドレスが172.16.1.1のマネージャのアクセスを許可することになります。

注　意　**コミュニティ名は最大20 個まで設定できます。**

authenTrap

キーワード **snmpconfファイル**

書　式　**authenTrap　{on｜off}**

デフォルト　**off**

解　説　Authentication違反トラップを送信するかどうかを設定します。
トラップを送信させたい場合には、「on」を指定します。

注　意　**Authentication違反トラップは、下記の事象で発生します。**
① SNMPのリクエストパケットのコミュニティ名が設定と一致しない。
② SNMPのリクエストパケットのコミュニティ名は一致するが、マネージャのIPアドレスが設定と一致しない。

linkTrap

キーワード **snmpconfファイル**

書　式　**linkTrap　{on｜off}**

デフォルト　**off**

解　説　linkUp/Downトラップを送信するか どうかを設定します。
トラップを送信させたい場合には、「on」を指定します。

linktrapifs

キーワード **snmpconfファイル**

書　式　**linktrapifs　{<論理インタフェース名>｜<論理インタフェース名>}　．．．**

例　**linktrapifs en0 en1**
linktrapifs P1-1PRI P1-2PRI P1-3PRI
linktrapifs hsd1 hsd2 hsd3

解　説　linkUp/Downを検出したらトラップを発生させる論理インタフェース名を設定します。例のように複数の論理インタフェース名を列挙することができます。

論理インタフェース名	説　　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
P1-＊PRI	拡張ボードスロット番号1とPRIポート番号の論理インタフェース名 ＊：PRIポート番号（1〜6）
hsd＊	高速ディジタル回線の論理インタフェース名（＊：1〜）

注　意　**linkTrapキーワードで、linkUp/Downトラップをonに設定しておく必要があります。**

5.10　usersファイル

本装置とISDN回線経由で接続（発信／着信）する接続相手の情報を設定します。
usersファイルの全体の構成は以下のようになっています。

```
%分類キーワード
        キーワード　パラメータ
        キーワード　パラメータ

%分類キーワード
        キーワード　パラメータ
        キーワード　パラメータ

%分類キーワード
        キーワード　パラメータ
        キーワード　パラメータ
                サブキーワード　　　　　パラメータ
```

まず分類キーワードを指定し、次に動作を指定するキーワードとそのパラメータを列挙します。
分類キーワードは先頭に「%」を付けて表します。
キーワードは分類キーワードから次の分類キーワードの間で有効です。キーワードの中には、サブキーワードを指定できるキーワードがあります。この場合もサブキーワードは、キーワードから次のキーワードの間で有効になります。

usersファイルで使用する、分類キーワードの一覧を**表5-5**、キーワード、サブキーワードの一覧を**表5-6**に示します。**表5-6**における「使用できる分類キーワード」の項目は、各キーワード、サブキーワードがどの分類キーワードで使用できるのか、を示しています。

表5-5　usersファイルの分類キーワード一覧

分類キーワード	機　能
%preset	着信時の認証が終了するまでの本装置の動作を設定する。
%default	接続相手に共通な設定項目を設定する。
%user	接続相手ごとの設定項目を設定する。

表5-6　usersファイルのキーワード／サブキーワード一覧

(1 / 2)

キーワード／サブキーワード	機　能	使用できる分類キーワード		
		%user	%default	%preset
remote_tel	接続相手の電話番号の設定	○		
accept_tel	着信で許可する電話番号の設定	○		
auto_disconnect	アイドル監視による回線自動切断を行うかどうかの設定	○	○	
idle_timeout	回線のアイドル監視時間の設定	○	○	
idle_ctl	アイドル監視を使用する条件の設定	○	○	
idle_timeout_in	着信時の回線のアイドル監視時間の設定	○	○	
idle_timeout_out	発信時の回線のアイドル監視時間の設定	○	○	
session_disconnect	連続接続時間による回線自動切断を行うかどうかの設定	○	○	
session_timeout	連続接続可能時間の設定	○	○	
connect_on_demand	回線自動接続機能を行うかどうかの設定	○	○	
accept_call	着信を受け付けるかどうかの設定	○	○	○
frame_type	発信時の回線属性の設定	○	○	
accept_frame_type	着信を許可する回線属性の設定			○
clid_auth	CLID認証を行うかどうかの設定	○	○	○
auth_request	接続相手に要求するPPP認証の設定	○	○	○
auth_accept	接続相手から受け入れるPPP認証の設定	○	○	○
local_name	PPP認証における本装置ユーザ名の設定	○	○	
local_passwd	PPP認証における本装置のパスワードの設定	○	○	
remote_name	PPP認証における接続相手のユーザ名の設定	○		
remote_passwd	PPP認証における接続相手のパスワードの設定	○		
protocol	動作プロトコルの設定	○	○	○
multi_connect	同一ユーザ名での複数同時接続に関する設定	○	○	
mp_port_min	MP/BACPで発信時に最初に接続するリンク数の設定	○	○	
mp_port_max	MP/BACPで最大接続リンク数の設定	○	○	
bod	MP/BACPでBOD機能を使用するかどうかの設定	○	○	
bod_ctl	BOD機能を動作させる条件の設定	○	○	
bod_add_rate	BODでリンクを増加させるレート(%)の設定	○	○	
bod_del_rate	BODでリンクを減少させるレート(%)の設定	○	○	
bod_sample_time	BODでレートを算出する平均化時間の設定	○	○	
cb	コールバックを使用するかどうかの設定	○	○	
cb_type	コールバック方式の設定	○	○	
cb_mode	コールバックモードの設定	○	○	
dns1	プライマリDNSサーバの動作モードの設定	○	○	
dns1_addr	プライマリDNSサーバのアドレスの設定	○	○	
dns2	セカンダリDNSサーバの動作モードの設定	○	○	
dns2_addr	セカンダリDNSサーバのアドレスの設定	○	○	
wins1	プライマリWINSサーバの動作モードの設定	○	○	
wins1_addr	プライマリWINSサーバのアドレスの設定	○	○	
wins2	セカンダリWINSサーバの動作モードの設定	○	○	
wins2_addr	セカンダリWINSサーバのアドレスの設定	○	○	
ippool	使用するIPプール番号の設定	○	○	
interface	接続相手に対するインタフェースの設定	○		
ppp	IPCPにおけるIPアドレスのネゴに関する設定 （interfaceキーワードのサブキーワード）	○		
filter	IPフィルターの設定 （interfaceキーワードのサブキーワード）	○		

表5-6　usersファイルのキーワード／サブキーワード一覧

(2 / 2)

キーワード／サブキーワード	機　能	使用できる分類キーワード		
		%user	%default	%preset
access	IPパケットの入力フィルタの設定（interfaceキーワードのサブキーワード）	○		
outputfil	IPパケットの出力フィルタの設定（interfaceキーワードのサブキーワード）	○		
destination	接続相手に対するルーティング情報の設定	○		
filter	IPフィルターの設定（destinationキーワードのサブキーワード）	○		
port	発信と着信で使用するポートの設定	○	○	

%user

分類キーワード　　**usersファイル**

書　式　　**%user**

解　説　　ISDN回線を経由して接続する接続相手の各種設定情報をキーワード、サブキーワードを使用して設定します。複数の接続相手の設定を行う場合、各接続相手の設定項目の先頭に「%user」を記述します。その後、次の「%user」が現れるまでの間のキーワード、サブキーワードで設定した内容が、その接続相手の情報になります。
キーワードのデフォルト値を使用する場合には、設定する必要はありません。
また「%default」に記述したキーワードの内容は自動的に参照されますので、その設定内容を使用する場合には設定する必要はありません。

参　照　　**「3章　3.2.3 」「 4章　4.1、4.2、4.4」**

%default

分類キーワード　　**usersファイル**

書　式　　**%default**

解　説　　この%default分類キーワードに記述されているキーワードは、全ての%userエントリに参照されます。したがって複数の%userエントリで共通に設定するキーワードがある場合、この%default分類キーワードに設定することによって、各%user分類キーワードに設定する手間が省けます。

参　照　　**「3章　3.2.3」**

%preset

分類キーワード **usersファイル**

書　式　**%preset**

解　説　着信時に、ISDN回線の着信から接続相手が特定できるまで（usersファイルのその接続相手の%userのエントリが見つかるまで、あるいは%userのエントリがみつからずにRADIUS認証を行うまで）の間の動作条件を設定します。
CLID認証を行う場合には、ISDN回線から着信した時点で接続相手を特定できるため、ISDN回線接続後のPPPの接続フェーズは、その接続相手の「%user」エントリに記述された設定内容で動作します。一方CLID認証を行わずにPPP認証のみを行う場合、PPP認証終了後に接続相手を特定することになりますので、PPP認証までの動作条件（auth_request、auth_acceptなど）を、この%preset分類キーワードで記述する必要があります。

参　照　**「3章　3.2.3」「4章　4.1、4.2」**

remote_tel

キーワード **usersファイル**

書　式　**remote_tel　<電話番号>**[*__<サブアドレス>__]

例　1　**remote_tel 043-222-3333**
例　2　**remote_tel 012-345-6789*111**

解　説　接続相手の電話番号を設定します。この電話番号は発信時には接続先の電話番号として、また着信時にCLID認証を行う場合にチェックする電話番号として使用されます。
<電話番号>は、区切り記号として「-」（ハイフン）を使用できます。
<サブアドレス>を指定する場合には、例2のように電話番号の後ろに「*」をつけて、その後ろにサブアドレスを記述します。サブアドレスには英数字を使用でき、最大19文字です。
1つのユーザ（1つの%userエントリ）で設定できる電話番号は、remote_tel、accept_telあわせて8つまでです。

関　連　**accept_telキーワード**

accept_tel

キーワード **usersファイル**

書　式　**accept_tel　<電話番号>[*<サブアドレス>]**

例　**accept_tel 012-345-6789**

解　説　着信時CLID認証を行う場合に、チェックする電話番号として使用されます。発信時の相手電話番号と、着信時に通知される相手電話番号が異なる場合には、発信時の電話番号をremote_telキーワードで、着信時にチェックする電話番号をaccept_telキーワードで設定します。
<電話番号>は、区切り記号として「-」（ハイフン）を使用できます。
<サブアドレス>を指定する場合には、電話番号の後ろに「*」をつけて、その後ろにサブアドレスを記述します。サブアドレスには英数字を使用でき、最大19文字です。

関　連　**remote_telキーワード**

auto_disconnect

キーワード **usersファイル**

書　式　**auto_disconnect　{on｜off}**

デフォルト　**on**

解　説　アイドル監視による回線自動切断を行うかどうかを設定します。「on」に設定した場合、idle_timeoutで設定した時間アイドル状態(データが流れていない状態)を検出すると、ISDN回線を切断します。

関　連　**idle_timeoutキーワード、idle_ctlキーワード、idle_timeout_inキーワード、idle_timeout_outキーワード**

参　照　**「4章　4.4.6」**

idle_timeout

キーワード **usersファイル**

書　式　**idle_timeout　<タイムアウト時間>**

例　**idle_timeout 60**

デフォルト　**120**

解　説　アイドル監視による回線自動切断を行う際のタイムアウト時間を設定します。
単位は秒で、設定値の範囲は、5〜100000(秒)です。
このidle_timeoutの設定は、auto_disconnectが「on」の場合に有効になります。

関　連　**auto_disconnectキーワード、idle_ctlキーワード、**
idle_timeout_inキーワード、idle_timeout_outキーワード

参　照　**「4章　4.4.6」**

idle_ctl

キーワード **usersファイル**

書　式　**idle_ctl　{both｜in｜out}**

デフォルト　**both**

解　説　アイドル監視による回線自動切断を、発信時または着信時に行うかどうかを設定します。
このidle_ctlの設定は、auto_disconnectが「on」の場合に有効になります。

- both :　発信時、着信時ともアイドル監視による回線自動切断を行う。
- in　:　着信時のみアイドル監視による回線自動切断を行い、発信時は行わない。
- out　:　発信時のみアイドル監視による回線自動切断を行い、着信時は行わない。

関　連　**auto_disconnectキーワード、idle_timeoutキーワード、**
idle_timeout_inキーワード、idle_timeout_outキーワード

参　照　**「4章　4.4.6」**

idle_timeout_in

キーワード **usersファイル**

書　式　**idle_timeout_in　<タイムアウト時間>**

例　**idle_timeout_in 90**

解　説　着信時に、アイドル監視による回線自動切断を行う際のタイムアウト時間を設定します。
単位は秒で、設定値の範囲は、5〜100000(秒)です。
このidle_timeout_inの設定は、auto_disconnectが「on」でかつidle_ctlキーワードが「both」または「in」の場合に有効になります。
このidle_timeout_inの設定がされていない場合、着信時のアイドル監視のタイムアウト時間には、idle_timeoutの値が使用されます。

関　連　**auto_disconnectキーワード、idle_timeoutキーワード、idle_ctlキーワード、idle_timeout_outキーワード**

参　照　**「4章　4.4.6」**

idle_timeout_out

キーワード **usersファイル**

書　式　**idle_timeout_out　<タイムアウト時間>**

例　**idle_timeout_out 20**

解　説　発信時に、アイドル監視による回線自動切断を行う際のタイムアウト時間を設定します。
単位は秒で、設定値の範囲は、5〜100000(秒)です。
このidle_timeout_outの設定は、auto_disconnectが「on」でかつidle_ctlキーワードが「both」または「out」の場合に有効になります。
このidle_timeout_outの設定がされていない場合、発信時のアイドル監視のタイムアウト時間には、idle_timeoutの値が使用されます。

関　連　**auto_disconnectキーワード、idle_timeoutキーワード、idle_ctlキーワード、idle_timeout_inキーワード**

参　照　**「4章　4.4.6」**

session_disconnect

キーワード **usersファイル**

書　式　　**session_disconnect　{on｜off}**

デフォルト　**off**

解　説　　連続接続時間による回線自動切断を行うかどうかを設定します。「on」に設定した場合、session_timeoutで設定した時間が経過した時点で、ISDN回線を切断します。

関　連　　**session_timeoutキーワード**

参　照　　**「4章　4.4.6」**

session_timeout

キーワード **usersファイル**

書　式　　**session_timeout　<タイムアウト時間>**

例　　　　**session_timeout 1800**

デフォルト　**3600**

解　説　　連続接続時間による回線自動切断を行う際のタイムアウト時間を設定します。単位は秒で、設定値の範囲は、5～100000(秒)です。
このsession_timeoutの設定は、session_disconnectが「on」の場合に有効になります。

関　連　　**session_disconnectキーワード**

参　照　　**「4章　4.4.6」**

connect_on_demand

キーワード **usersファイル**

書　式　**connect_on_demand　{on｜off}**

デフォルト　**off**

解　説　connect_on_demandが「on」の場合、interfaceキーワードあるいはdestinationキーワードで設定された宛先アドレスのパケットを検出した場合、本装置が自動的に発信し、接続に成功すると、その宛先アドレスに対するパケットのルーティングが行われます。

accept_call

キーワード **usersファイル**

書　式　**accept_call　{on｜off}**

デフォルト　**on**

解　説　ISDN回線からの着信を受け付けるかどうかを設定します。「off」に設定すると、着信は拒否されます。
%preset分類キーワードにおいてaccept_callを「off」に設定すると、すべてのISDNの着信は拒否されます。
一方%user分類キーワードにおいてaccept_callを「off」に設定した場合、その接続相手のみ着信は拒否されます。この時accept_callがチェックされるタイミングは、CLID認証を行う場合には、ISDN回線から着信しその着信を受け付ける前です。またCLID認証を使用せずにPPP認証を行う場合には、PPP認証を行った後です。

clid_auth

キーワード **usersファイル**

書　式　**clid_auth　{off｜may｜must}**

デフォルト　**off**

解　説

着信時のCLID認証（相手電話番号のチェックによる認証）の動作モードを設定します。

%preset分類キーワードに設定した場合、以下のように動作します。

off　：ISDN回線の着信時、相手電話番号のチェックを行いません。属性の一致するすべてのISDNの着信は許可され、PPPの接続フェーズが実行されます。

may　：ISDN回線からの着信時に、電話番号のチェックを行います。もし相手電話番号と一致する電話番号が設定されているユーザエントリ（本装置のusersファイルにremote_tel/accept_telキーワードを含む%userエントリ、またはRADIUS認証サーバのusersファイルに相手電話番号で登録したエントリ）が存在した場合、ISDNの着信を許可します。この場合、以後のPPPの接続フェーズは、ユーザエントリの内容に従って動作します。
一致するユーザエントリが見つからなかった場合でも、ISDNの着信は許可されPPPの接続フェーズが実行されますが、PPP認証が終了するまで%preset分類キーワードの設定内容で動作します。

must　：ISDN回線からの着信時に、電話番号のチェックを行います。この場合には、相手電話番号と一致するユーザエントリ（本装置のusersファイルにremote_tel/accept_telキーワードを含む%userエントリ、またはRADIUS認証サーバのusersファイルに相手電話番号で登録したエントリ）が見つからなかった場合には、ISDNの着信を拒否します。ユーザエントリが見つかった場合には、ISDNの着信を許可し、以後のPPPの接続フェーズは、ユーザエントリの内容に従って動作します。

%user分類キーワードに設定した場合、PPP認証が成功した後にCLID認証を行います。

off　：相手電話番号のチェックを行いません。

may／must：相手電話番号のチェックを行い、一致しない場合には、その接続を切断します。

注　意　**RADIUS認証サーバを使用してCLID認証を行う場合は、本装置のradiusファイルの設定が必要です。**

参　照　**「4章　4.4.2」**

auth_request

キーワード **usersファイル**

書　式　**auth_request　{none｜pap｜chap｜either｜pap-｜chap-｜either-}**

デフォルト　**none**

解　説　PPP認証で相手を認証する場合に、相手に要求する認証プロトコルを設定します。

none　：PPP認証を要求しない。
pap　：発信時、着信時ともにPAPを要求する。
chap　：発信時、着信時ともにCHAPを要求する。
either　：発信時、着信時ともにCHAPを要求し、それが相手に受け入れられなかった場合、改めてPAPを要求する。
pap-　：着信時のみPAPを要求し、発信時には認証を要求しない。
chap-　：着信時のみCHAPを要求し、発信時には認証を要求しない。
either-　：着信時のみCHAPを要求し、それが相手に受け入れられなかった場合、改めてPAPを要求する。発信時には認証を要求しない。

参　照　**「4章　4.4.1、4.4.3」**

auth_accept

キーワード **usersファイル**

書　式　**auth_accept　{none｜pap｜chap｜remote｜pap-｜chap-｜remote-}**

デフォルト　**none**

解　説　PPP認証で相手から認証される場合、受け入れる認証プロトコルを設定します。

none　：PPP認証は受け入れない。
pap　：発信時、着信時ともPAPを受け入れる。
chap　：発信時、着信時ともCHAPを受け入れる。
remote　：発信時、着信時とも相手が要求するPAPあるいはCHAPあるいはPPP認証なしを受け入れる。
pap-　：発信時のみPAPを受け入れ、着信時はPPP認証は受け入れない。
chap-　：発信時のみCHAPを受け入れ、着信時はPPP認証は受け入れない。
remote-　：発信時のみ相手が要求するPAPあるいはCHAPあるいはPPP認証なしを受け入れ、着信時はPPP認証は受け入れない。

参　照　**「4章　4.4.1、4.4.3」**

local_name

キーワード **usersファイル**

書　式　　**local_name　<ユーザ名>**

例　　**local_name myname**

解　説　　PPP認証で使用する自局ユーザ名を設定します。英数字で最大64文字です。

参　照　　**「4章　4.4.1」**

local_passwd

キーワード **usersファイル**

書　式　　**local_passwd　<パスワード>**

例　　**local_passwd mypasswd**

解　説　　PPP認証で使用する自局パスワードを設定します。英数字で最大32文字です。

参　照　　**「4章　4.4.1」**

remote_name

キーワード **usersファイル**

書　式　　**remote_name　<ユーザ名>**

例　　**remote_name yourname**

解　説　　PPP認証で使用する相手局ユーザ名を設定します。英数字で最大64文字です。

参　照　　**「4章　4.4.1」**

remote_passwd

キーワード **usersファイル**

書　式　remote_passwd　<パスワード>

例　remote_passwd yourpasswd

解　説　PPP認証で使用する相手局パスワードを設定します。英数字で最大32文字です。

参　照　「4章　4.4.1」

protocol

キーワード **usersファイル**

書　式　protocol　{ppp｜mp｜bacp}

デフォルト　ppp

解　説　使用する動作プロトコルを設定します。

ppp　：PPPを使用する。
mp　：MPを使用する。
bacp　：BACPを使用する。

注　意　**protocolキーワードは、%presetと%user分類キーワードで設定することができますので以下の点に注意してください。**

・%presetのprotocol設定
本装置が着信した時に受け入れるプロトコルを設定します。
ppp　：PPPのみ受け入れる。
接続相手からMPまたはBACPで要求された場合はそれを拒否して、PPPで接続する。
mp　：PPPとMPのみ受け入れる。
接続相手からBACPで要求された場合はそれを拒否して、PPPまたはMPで接続する。
bacp　：PPP、MP、BACPを受け入れる。

・%userのprotocol設定

本装置が発信する時に使用するプロトコルを設定します。

ppp　：PPPを使用する。

mp　：MPを使用する。
接続相手がMPを受け入れない場合はPPPで接続する。

bacp　：BACPを使用する。
接続相手がBACPを受け入れない場合はMPまたはPPPで接続する。

ただし、着信時にCLID認証で接続相手を特定した場合は%presetのprotocol設定と同様に、着信した時に受け入れるプロトコル設定としても使用されます。
また、以下の設定例のように、上記%presetのprotocol設定と%userのprotocol設定が異なる場合は、相手ルータから先に着信した場合は、%presetのprotocolの設定が有効になりMPで接続します。
本装置が先に発信した場合は、%userのprotocolの設定が有効になりPPPで接続されますので注意が必要です。

```
%preset            # 着信時のプロトコル設定
      protocol   mp

%user              # 発信時のプロトコル設定
      protocol  PPP
```

multi_connect

キーワード　　　　usersファイル

書　式　multi_connect　{on｜off}

デフォルト　off

解　説　同じユーザ名で、同時に複数接続を可能にするかを設定します。

on ： 複数接続可能。
off ： 複数接続不可。

注　意　multi_connect「on」は以下の場合に使用してください。

・本装置が着信する場合
・本装置から接続相手に対してIPアドレスを割り当てる場合
・ 動作プロトコルがPPPの場合

上記以外の場合には、動作は保証されません。

mp_port_min

キーワード **usersファイル**

書　式　**mp_port_min　<リンク数>**

例　**mp_port_min 2**

デフォルト　**1**

解　説　MPまたはBACPで発信する場合に、発信時に同時に接続するリンク数（チャネル数）を設定します。
設定範囲は1～8です。
mp_port_minキーワードを2以上に設定した場合、発信時に2本目以降の接続に失敗した場合、あるいは設定値どおりにリンクが接続された状態で接続相手からリンクが切断された場合には、再接続は行いません（ただしBOD機能が動作していれば転送レートに応じて再度接続する場合はあります）。
またBOD機能を使用している場合、mp_port_minキーワードで設定したリンク数以下には、リンク数を削除することはありません。ただし接続相手から切断された場合には、設定値よりも少ないリンク数になることはあります。

参　照　**「4章　4.4.4」**

mp_port_max

キーワード **usersファイル**

書　式　**mp_port_max　<リンク数>**

例　**mp_port_max 4**

デフォルト　**2**

解　説　MPまたはBACPを使用している場合に接続できる最大リンク数（チャネル数）を設定します。
設定範囲は1～8です。
mp_port_maxキーワードで設定したリンク数を超えるリンク数になることはありません。もし接続相手から着信した場合には、その着信を拒否します。

参　照　**「4章　4.4.4」**

bod

キーワード **usersファイル**

書　式　**bod　{on｜off}**

デフォルト　**on**

解　説　MPまたはBACPを使用している場合に、BOD機能（回線上の転送レートに応じてリンク数を増加／減少させる）を使用するかどうかの設定を行います。「on」に設定すると、本装置が転送レートに応じてリンク数の増減を行います。この時の動作については、キーワードbod_ctl、bod_add_rate、bod_del_rate、bod_sample_timeなどで詳細に指定することができます。

参　照　**「4章　4.4.4」**

bod_ctl

キーワード **usersファイル**

書　式　**bod_ctl　{out｜in｜both}**

デフォルト　**out**

解　説　MPまたはBACPを使用している場合に、BOD機能を動作させる条件を設定します。

out　：1本目のリンクを本装置が発信した場合BOD機能が動作する。
in　：1本目のリンクを本装置が着信した場合BOD機能が動作する。
both　：1本目のリンクを本装置が発信した場合、着信した場合ともにBOD機能が動作する。

参　照　**「4章　4.4.4」**

bod_add_rate

キーワード **usersファイル**

書　式　**bod_add_rate　<レート>**

例　**bod_add_rate 60**

デフォルト　**70**

解　説　BOD機能を使用している場合に、転送レートが上がってきた時にリンクを増加させるレートを%で設定します。リンク増加を行う転送レートRは、以下の式で算出されます。設定範囲は10〜90です。

R(Kbps) =(N(現在のリンク数)ー1) × 64(Kbps)+ 64(Kbps)× bod_add_rate(%)

例えば現在リンク数が1の状態で、bod_add_rateが60に設定されている場合、

R = (1ー1)× 64 +64× 0.60 = 38.4（Kbps）

となり、これ以上転送レートが上がるとリンクが1本追加されます。

関　連　**bod_del_rate**

参　照　**「4章　4.4.4」**

注　意　**bod_add_rateは必ずbod_del_rateより大きい値を設定してください。もしbod_del_rateをbod_add_rateと等しいか、bod_add_rateより大きい値を設定するとリンクの追加/削除を繰り返してしまう可能性があります。**
また、bod_add_rateとbod_del_rateの差が小さい場合にも同様の可能性がありますので注意が必要です。

bod_del_rate

キーワード **usersファイル**

書　式　**bod_del_rate　<レート>**

例　**bod_del_rate 40**

デフォルト　**30**

解　説　BOD機能を使用している場合に、転送レートが下がってきた時にリンクを減少させるレートを%で設定します。リンク減少を行う転送レートRは、以下の式で算出されます。

R(Kbps)＝(N(現在のリンク数)－２)×64(Kbps)＋64(Kbps)×bod_del_rate(%)

例えば現在のリンク数が２の状態で、bod_del_rateが40に設定されている場合、

R(Kbps) ＝ (2－2)× 64 ＋ 64 × 0.40 ＝ 25.6(Kbps)

となり、これ以上転送レートが下がると、リンクが１本減少されます。

関　連　**bod_add_rate**

参　照　**「4章　4.4.4」**

bod_sample_time

キーワード **usersファイル**

書　式　**bod_sample_time　<サンプル時間>**

例　**bod_sample_time 20**

デフォルト　**15**

解　説　BOD機能を使用する場合に、転送レートを算出するための平均化時間を秒数で指定します。ここに設定された時間の平均転送レートがbod_add_rate、bod_del_rateにおける転送レートとして使用されます。設定範囲は5～60（秒）です。

この時間を短くすると、転送レートの変動に対するリンクの増減の反応が速くなりますが、一時的な高負荷が発生した場合でもリンクの増加が発生してしまう可能性がありますので、注意が必要です。

参　照　**「4章　4.4.4」**

dns1

キーワード **usersファイル**

書　式　**dns1　{none｜accept}**

デフォルト　**none**

解　説　PPPのIPCPプロトコルで行われるプライマリDNSサーバアドレスのネゴシエーションの動作を指定します。

none　：相手からプライマリDNSサーバアドレスの割り当てを要求された場合、受け付けない。

accept：相手からプライマリDNSサーバアドレスの割り当てを要求された場合、dns1_addrキーワードで指定されたアドレスを割り当てる。

関　連　**dns1_addrキーワード**

dns1_addr

キーワード **usersファイル**

書　式　**dns1_addr　<プライマリDNSサーバアドレス>**

例　**dns1_addr 172.31.0.1**

解　説　PPPのIPCPプロトコルで行われるプライマリDNSサーバアドレスのネゴシエーションの際、相手に割り当てるプライマリDNSサーバアドレスの値を設定します。

関　連　**dns1キーワード**

dns2

キーワード **usersファイル**

書　式　**dns2　{none｜accept}**

デフォルト　**none**

解　説　PPPのIPCPプロトコルで行われるセカンダリDNSサーバアドレスのネゴシエーションの動作を指定します。

none　：　相手からセカンダリDNSサーバアドレスの割り当てを要求された場合、受け付けない。

accept　：　相手からセカンダリDNSサーバアドレスの割り当てを要求された場合、dns2_addrキーワードで指定されたアドレスを割り当てる。

関　連　**dns2_addrキーワード**

dns2_addr

キーワード **usersファイル**

書　式　**dns2_addr　<セカンダリDNSサーバアドレス>**

例　**dns2_addr 172.31.0.2**

解　説　PPPのIPCPプロトコルで行われるセカンダリDNSサーバアドレスのネゴシエーションの際、相手に割り当てるセカンダリDNSサーバアドレスの値を設定します。

関　連　**dns2キーワード**

wins1

キーワード **usersファイル**

書　式　**wins1　{none｜accept}**

デフォルト　**none**

解　説　PPPのIPCPプロトコルで行われるプライマリWINSサーバアドレスのネゴシエーションの動作を指定します。

none　：相手からプライマリWINSサーバアドレスの割り当てを要求された場合、受け付けない。

accept：相手からプライマリWINSサーバアドレスの割り当てを要求された場合、wins1_addrキーワードで指定されたアドレスを割り当てる。

関　連　**wins1_addrキーワード**

wins1_addr

キーワード **usersファイル**

書　式　**wins1_addr　<プライマリWINSサーバアドレス>**

例　**wins1_addr 172.31.0.3**

解　説　PPPのIPCPプロトコルで行われるプライマリWINSサーバアドレスのネゴシエーションの際、相手に割り当てるプライマリWINSサーバアドレスの値を設定します。

関　連　**wins1キーワード**

wins2

キーワード **usersファイル**

書　式　**wins2　{none｜accept}**

デフォルト　**none**

解　説　PPPのIPCPプロトコルで行われるセカンダリWINSサーバアドレスのネゴシエーションの動作を指定します。

none　：　相手からセカンダリWINSサーバアドレスの割り当てを要求された場合、受け付けない。

accept：　相手からセカンダリWINSサーバアドレスの割り当てを要求された場合、wins2_addrキーワードで指定されたアドレスを割り当てる。

関連　**wins2_addrキーワード**

wins2_addr

キーワード **usersファイル**

書　式　**wins2_addr　<セカンダリWINSサーバアドレス>**

例　**wins2_addr 172.31.0.4**

解　説　PPPのIPCPプロトコルで行われるセカンダリWINSサーバアドレスのネゴシエーションの際、相手に割り当てるセカンダリWINSサーバアドレスの値を設定します。

関　連　**wins2キーワード**

ippool

キーワード **usersファイル**

書　式　**ippool　<IPプール番号>**

例　**ippool 3**

デフォルト　**1**

解　説　IPプールを使って接続相手にIPアドレスを割り当てる場合に、何番のプールを使用するかを設定します。
設定値の範囲は、0および1～16です。

IPプールは、ippoolファイルに登録します。ippoolファイルには、1～16番までのIPプールを登録することができます。
このippoolキーワードでは、ippoolファイルに登録されているIPプールに対応するIPプール番号（1～16）を設定します。
また、0を設定すると、ippoolファイルに登録されているすべてのIPプールから空いているIPアドレスを検索して、空いているIPアドレスを割り当てることができます。

関連　**ippoolファイル**

参　照　**「4章　4.4.7」**

cb

キーワード **usersファイル**

書　式　**cb　{none｜request｜accept}**

デフォルト　**none**

解　説　コールバックを使用するかどうかを設定します。

none　：コールバックは使用しない。
request　：コールバック要求を発行する。
accept　：コールバック要求を受け入れて、コールバックする。

参　照　**「4章　4.4.5」**

5章　セットアップファイル・リファレンス

cb_type

キーワード **usersファイル**

書　式　**cb_type　{cbcp｜isdn}**

デフォルト　**cbcp**

解　説　使用するコールバック方式を設定します。cbキーワードがnoneの場合は意味がありません。

cbcp　：CBCP
isdn　：無課金コールバック

注　意　**無課金コールバックは本装置独自の方式であるため、本装置間の接続時に使用してください。**

参　照　**「4章　4.4.5」**

cb_mode

キーワード 　　　　　　　　　　　　　　　　**usersファイル**

書　式　**cb_mode　{may｜must}**

デフォルト　**must**

解　説　コールバックの動作モードを設定します。
cb_typeキーワードがcbcpの場合有効になります。

cbキーワード	cb_type キーワード	cb_mode キーワード	意　味
request	cbcp	may	コールバック要求を発行して、接続相手から拒否された場合は、 コールバック要求せずに通常の発信で接続します。
		must	コールバック要求を発行して、接続相手から拒否された場合は、発信失敗として接続しません。
accept		may	相手がコールバック要求を発行してこなかった場合は、通常の着信で接続します。
		must	相手がコールバック要求を発行してこなかった場合は、着信を拒否します。

参　照　**「4章　4.4.5」**

port

キーワード 　　　　　　　　　　　　　　　　**usersファイル**

書　式　**port　<拡張ボードスロット番号>/<ポート番号>**

例　**port 1/6**

解　説　発信と着信で使用するポートを設定します。
本キーワードが設定されているユーザに発信する場合は、指定したポートから発信します。もし、指定したポートがすべて使用中であれば、発信に失敗します。
本キーワードが設定されているユーザから着信した場合は、指定したポートからのみ許可します。もし、指定したポート以外から着信した場合は、ユーザの認証後に切断します。
本キーワードを設定していないユーザの場合は、ポートによる発信、着信の制限を行いません。

interface

キーワード **usersファイル**

書　式　**interface　<論理インタフェース名>[/<自局IPアドレス>]　<相手IPアドレス> <属性>**

例　1　**interface isdn0128.30.0.1 unnumbered**
例　2　**interface isdn0/172.31.0.1 172.31.0.2 numbered**
例　3　**interface isdn0　*　unnumbered**

解　説　interfaceキーワードでは、接続する相手との間でIPが使用するインタフェースの条件を設定します。

<論理インタフェース名>　IPで使用するISDNの論理インタフェース名を指定します。必ず「isdn0」を設定してください。

<自局IPアドレス>　論理インタフェースに固有の自局IPアドレスを割り当てる場合、対応する自局IPアドレスを設定します。省略した場合には、本装置のホスト名に対応するIPアドレスが割り当てられます。

<相手IPアドレス>　接続相手がインタフェースにIPアドレスを持つ場合には、そのIPアドレスを設定します。接続相手がインタフェースにIPアドレスを持たない場合には、接続相手自身のIPアドレスを設定します。
端末型接続においては、接続相手のIPアドレスを本装置から割り当てる場合があり、その場合にはあらかじめ相手IPアドレスはわかりません。この場合には「*」を設定します。「*」を設定した場合には、IPCPのアドレスネゴシエーションで相手IPアドレスが決定した時点で本装置がその値を設定します。

<属性>　この論理インタフェースに固有のIPアドレスを割り当てる場合には、「numbered」を設定します。固有のIPアドレスを割り当てない場合には、「unnumbered」を設定します。

interfaceキーワードでは、サブキーワードでIPフィルタやPPPのアドレスネゴシエーションのオプションを設定することができます。サブキーワードはinterfaceキーワードに続けて次の行から設定します。

関　連　**pppサブキーワード、filterサブキーワード、accessサブキーワード**

参　照　**「4章　4.1、4.2」**

ppp

サブキーワード **usersファイル**

書　式　**ppp address <モード> <自局アドレス> <相手アドレス>**

例　1　**ppp address on * ***
例　2　**ppp address on 172.31.0.1 192.168.0.1**
例　3　**ppp address on * 255.255.255.255**

解　説　pppサブキーワードは、interfaceキーワードのサブキーワードです。
PPPのIPCPプロトコルで行われるアドレスネゴシエーションの動作を指定します。

<モード>　IPCPのアドレスネゴシエーションにおいて、自局IPアドレスを送信するかどうかを設定します。「on」の場合自局IPアドレスを送信しますが、「off」の場合送信しません。

<自局アドレス><モード>が「on」の場合に、送出する自局アドレスを設定します。「*」を設定した場合、interfaceキーワードで指定した自局IPアドレスが使用されます。

<相手アドレス>　アドレスネゴシエーションにおける相手IPアドレスを設定します。以下の4種類の設定値があります。

(A)255.255.255.255　：相手が通知してきたIPアドレスを使用します。
(B)255.255.255.254　：本装置のIPプールのIPアドレスを使用します。
(C)上記以外のIPアドレス：設定されたIPアドレスを使用します。
(D)*　：interfaceキーワードで指定した相手局IPアドレスを使用します。

(B)、(C)、(D)の場合に、アドレスネゴシエーションで相手からIPアドレスの割り当てを要求された場合、その値を割り当てます。

filter

サブキーワード **usersファイル**

書　式　**filter　<フィルタ名>**

例　**filter telFIL**

解　説　filterは、interfaceキーワードのサブキーワードです。
論理インタフェースに直結したセグメント宛てのパケットに対するフィルタをかけたい場合、その条件を設定します。指定したフィルタ条件に一致したパケットのみが、そのセグメントにフォワーディングされます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

注　意　**フィルタが適用されるのは、この論理インタフェースに直結したセグメント宛てのパケットです。この論理インタフェースを経由して接続された先のセグメント宛てのフィルタを指定する場合には、destinationキーワードに設定してください。**

access

サブキーワード **usersファイル**

書　式　**access　{include｜exclude}　<フィルタ名>**

例　1　**access include ftpFIL**
例　2　**access exclude telFIL**

解　説　accessは、interfaceキーワードのサブキーワードです。
論理インタフェースに入力フィルタをかけたい場合、その条件を設定します。指定したフィルタ条件に一致したパケットのみ通過させたり、反対にフィルタに一致したパケットを廃棄させたりすることができます。入力フィルタの処理はパケットの受信処理で行われますので、ここで廃棄されたパケットは、フォワーディングされることはありません。
また、本装置あてのパケットもフィルタすることができますので、本装置への不正アクセスを防止することもできます。

「include」は、フィルタに一致したパケットのみを通過させる場合に指定します。
「exclude」は、フィルタに一致したパケットを廃棄させる場合に指定します。
「include」と「exclude」の両方とも指定した場合には、「include」のフィルタに一致せず、かつ「exclude」のフィルタに一致したパケットのみが廃棄され、それ以外のパケットはすべて通過します。

<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

outputfil

サブキーワード **usersファイル**

書　式　**outputfil　<フィルタ名>**

例　**outputfil telFIL**

解　説　outputfilは、interfaceのキーワードのサブキーワードです。
論理インタフェースに出力フィルタをかけたい場合、その条件を設定します。
指定したフィルタ条件に一致したパケットのみが出力されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

destination

キーワード **usersファイル**

書式　**destination　<宛先IPアドレス>/<マスク>　via　<経由ルータIPアドレス> <メトリック>**

例　1　**destination 128.30.0.0/net via 128.30.0.1 2**
例　2　**destination 172.31.1.0/24 via 128.30.0.1 2**
例　3　**destination 128.30.0.2/host via 128.30.0.1 2**

解　説　destinationキーワードで、接続相手に対するルーティング情報を設定します。
フォワーディングされるパケットの宛先IPアドレスが、**<宛先IPアドレス>/<マスク>**と比較され、一致した経路の**<経由ルータ>**にフォワーディングされます。
もし複数の経路と一致した場合には、最もマスク長の長い経路にフォワーディングされます。

<宛先アドレス>　デスティネーションのネットワークアドレス、またはホストアドレスを設定します。

<マスク>　**<宛先アドレス>**に対するマスクを設定します。フォワーディングされるパケットの宛先IPアドレスに、このマスクをかけた結果と、**<宛先アドレス>**が比較されます。

<経由ルータIPアドレス>　パケットをフォワーディングするルータのIPアドレスまたはホスト名を指定します。

<メトリック>　この経路のメトリックを10進数で設定します。範囲は1〜99です。

関　連　**filterサブキーワード**

参　照　**「4章　4.1、4.2」**

filter

サブキーワード **usersファイル**

書　式　**filter　<フィルタ名>**

例　**filter telFIL**

解　説　filterは、destinationキーワードのサブキーワードです。
destinationキーワードで設定したデスティネーション宛てのパケットに対するフィルタをかけたい場合、その条件を設定します。指定したフィルタ条件に一致したパケットのみが、そのデスティネーションにフォワーディングされます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

5.11 radiusファイル

RADIUS認証サーバ、RADIUSアカウントサーバとの通信に関するパラメータを設定します。
radiusファイルの全体の構成は以下のようになっています。

```
%radius_auth
        キーワード　パラメータ
        キーワード　パラメータ

%radius_acct
        キーワード　パラメータ
        キーワード　パラメータ
```

RADIUS認証サーバの設定は、%radius_auth分類キーワードの後に、キーワードで設定を行います。
RADIUSアカウントサーバの設定は%radius_acct分類キーワードの後に、キーワードで設定を行います。
分類キーワードは先頭に「%」を付けて表します。キーワードは分類キーワードから次の分類キーワードの間で有効です。
%radius_auth分類キーワード、%radius_acct分類キーワードで使用できるキーワードは一部を除いて共通です。

%radius_auth

分類キーワード 　　　　**radiusファイル**

書　式　　**%radius_auth**

解　説　　RADIUS認証サーバへの通信に関するパラメータを設定するキーワードの先頭に記述します。次に現れる分類キーワードの直前までのキーワード、あるいはファイルの最後までのキーワードが有効になります。

%radius_acct

分類キーワード 　　　　**radiusファイル**

書　式　　**%radius_acct**

解　説　　RADIUSアカウントサーバへの通信に関するパラメータを設定するキーワードの先頭に記述します。次に現れる分類キーワードの直前までのキーワード、あるいはファイルの最後までのキーワードが有効になります。

mode

キーワード **radiusファイル**

書　式　**mode　{on｜off}**

デフォルト　**off**

解　説　RADIUSサーバを使用するかどうかを指定します。
「on」に設定すると、RADIUSサーバに対するアクセスが可能になります。
「off」に設定すると、%radius_authに対するキーワードの場合、RADIUS認証サーバに対する認証要求を送信しません。また%radius_acctに対するキーワードの場合、RADIUSアカウントサーバに対するアカウント送信を行いません。

host1

キーワード **radiusファイル**

書　式　**host1　<IPアドレス>**

例　1　**host1 172.31.1.1**
例　2　**host1 horn**

解　説　RADIUSサーバのIPアドレスを、ドット記法またはhostsファイルに登録したホスト名で指定します。本装置では、RADIUSサーバを3つまで登録できます。
RADIUSサーバに対してアクセスする場合、まずhost1キーワードに設定されたホストにアクセスします。host1のホストからtimeoutキーワードで指定した時間待っても応答がなかった場合、host2キーワードに設定されたホストにアクセスします。host2のホストからも応答がなかった場合、さらにhost3キーワードに設定されたホストにアクセスします。host3からも応答がなかった場合、host1, host2, host3とラウンドロビン形式でアクセスします。応答があった場合は、次回のリクエストは応答があったホストにアクセスします。

host2

キーワード **radiusファイル**

書　式　**host2　<IPアドレス>**

例　1　**host2 172.31.1.2**
例　2　**host2 cornet**

解　説　RADIUSサーバのIPアドレスを、ドット記法またはhostsファイルに登録したホスト名で指定します。本装置では、RADIUSサーバを3つまで登録できます。
RADIUSサーバに対してアクセスする場合、まずhost1キーワードに設定されたホストにアクセスします。host1のホストからtimeoutキーワードで指定した時間待っても応答がなかった場合、host2キーワードに設定されたホストにアクセスします。host2のホストからも応答がなかった場合、さらにhost3キーワードに設定されたホストにアクセスします。host3からも応答がなかった場合、host1, host2, host3とラウンドロビン形式でアクセスします。応答があった場合は、次回のリクエストは応答があったホストにアクセスします。

host3

キーワード **radiusファイル**

書　式　**host3　<IPアドレス>**

例　1　**host3 172.31.1.3**
例　2　**host3 viola**

解　説　RADIUSサーバのIPアドレスを、ドット記法またはhostsファイルに登録したホスト名で指定します。本装置では、RADIUSサーバを3つまで登録できます。
RADIUSサーバに対してアクセスする場合、まずhost1キーワードに設定されたホストにアクセスします。host1のホストからtimeoutキーワードで指定した時間待っても応答がなかった場合、host2キーワードに設定されたホストにアクセスします。host2のホストからも応答がなかった場合、さらにhost3キーワードに設定されたホストにアクセスします。host3からも応答がなかった場合、host1, host2, host3とラウンドロビン形式でアクセスします。応答があった場合は、次回のリクエストは応答があったホストにアクセスします。

rtime

キーワード **radiusファイル**

書　式 **rtime　<リセットタイム>**

例 **rtime 300**

デフォルト **0（ディセーブル）**

解　説 RADIUSサーバに対するアクセスがhost1から他のホストへ移った場合に、host1に戻るまでの時間を秒数で指定します。設定値の範囲は、0～100000(秒)です。0の場合は、ディセーブルとなります。

RADIUSサーバに対してアクセスする場合、まずhost1キーワードに設定されたホストにアクセスします。host1のホストからtimeoutキーワードで指定した時間待っても応答がなかった場合、host2キーワードに設定されたホストにアクセスします。host2のホストからも応答がなかった場合、host3へとアクセスが移ります。host2, host3のどちらからか応答があった場合、次回以降のアクセスはそのホストが使用されます。アクセスがhost1から他のホストへ移ってからrtimeキーワードで指定した時間経過後、次のアクセスはhost1に戻ります。

port

キーワード **radiusファイル**

書　式 **port　<ポート番号>**

例 **port 1645**

デフォルト **1645（%radius_authの場合）**
1646（%radius_acctの場合）

解　説 RADIUSサーバのUDPのポート番号を、10進数で指定します。このキーワードを指定しない場合、デフォルトでRADIUS認証サーバでは1645、RADIUSアカウントサーバでは1646を使用します。
使用されるRADIUSサーバの設定と合わせてください。

key

キーワード **radiusファイル**

書　式　**key　<シークレット>**

例　**key router1pass**

解　説　本装置がRADIUSサーバにアクセスするためのシークレットキーを、英数字で指定します。使用されるRADIUSサーバの本装置に対する設定と合わせてください。

timeout

キーワード **radiusファイル**

書　式　**timeout　<タイムアウト値>**

例　**timeout 5**

デフォルト　**3**

解　説　RADIUSサーバからの応答がなかった場合のタイムアウト時間を秒数で指定します。
設定値の範囲は、1～255(秒)です。

retry

キーワード **radiusファイル**

書　式　**retry　<再送回数>**

デフォルト　**10**

解　説　RADIUSサーバに対するアクセスでタイムアウトが発生した場合の再送回数を指定します。
設定値の範囲は、1～255です。

retryキーワードで設定された回数再送してもRADIUSサーバからの応答がない場合、本装置は以下のように動作します。

- RADIUS認証サーバへのアクセスの場合、RADIUS認証失敗として動作します。
- RADIUSアカウントサーバへのアクセスの場合、本装置のコンソールにアカウント情報を出力し、そのアカウント情報は廃棄します。

chkauth

キーワード **radiusファイル**

書　式　**chkauth　{on｜off}**

デフォルト　**on**

解　説　RADIUSアカウントサーバに対してアカウント要求を送信した後に、本装置がその応答を受信した時に、受信フレームのauthenticatorをチェックするかどうかを設定します。onに設定するとチェックを行います。
通常この設定はonで使用します。
ただし、RADIUSサーバがLivingSton社のV1.16あるいはこのバージョンのRADIUSサーバをベースに開発されているRADIUSサーバの場合には、アカウント要求に対する応答に含まれているauthenticatorが正しく設定されていない場合があります。そのような場合、本装置はauthenticatorをチェックし、エラーと判断しアカウント要求を再送します。この結果RADIUSアカウントサーバに同じアカウントが複数記録されてしまいます。このような現象が発生する場合には、この設定をoffにすることによって回避することができます。

注　意　**このキーワードは、%radius_acct分類キーワードのみに有効です。**

set_session_id

キーワード **radiusファイル**

書　式　**set_session_id　{on｜off}**

デフォルト　**off**

解　説　RADIUS認証サーバに送信する認証要求（AccessRequest）パケットにAcct-Session-Idアトリビュートを入れるかどうかを設定します。
「on」に設定すると、Acct-Session-Idアトリビュートを入れて認証要求パケットを送信します。

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

base_session_id

キーワード **radiusファイル**

書　式　**base_session_id　{dec｜hex}**

デフォルト　**hex**

解　説　RADIUSアカウントサーバあるいはRADIUS認証サーバに送信するパケットに含まれるAcct-Session-IDアトリビュートの表示形式を設定します。
「hex」に設定すると、16進数表示になります。
「dec」に設定すると、10進数表示になります。

注　意　**このキーワードは、%radius_acct分類キーワードのみに有効です。**

stop_ignore

キーワード **radiusファイル**

書　式　**stop_ignore　{on｜off}**

デフォルト　**off**

解　説　本装置では、PPP認証以後のフェーズにおいて接続拒否あるいは接続失敗を検出した場合、RADIUSアカウントサーバに対してAcct-Status-TypeがSTOPのアカウントを送信します。このキーワードをonに設定することによって、このような接続失敗のアカウントを送信しないモードにすることができます。
このキーワードをonに設定しても、Acct-Status-TypeがSTARTのアカウントおよびそれに対応するSTOPのアカウントは送信されます。

注　意　**このキーワードは、%radius_acct分類キーワードのみに有効です。**

default_filter

キーワード **radiusファイル**

書　式　　**default_filter　<フィルタ名>**

設定例　　**default_filter telFIL**

解　説　　RADIUS認証において、RADIUS認証サーバから、「.filter」の拡張子があるFilter-Id attributeを指定されなかった場合には、このキーワードで指定したフィルタが使用されるinterfaceに設定されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

RADIUS認証サーバから「.filter」の拡張子があるFilter-Id attributeを指定された場合には、RADIUS認証サーバから受信したFilter-Id attributeが優先され、このキーワードで指定したフィルタは使用されません。

注　意　　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

default_include

キーワード **radiusファイル**

書　式　　**default_include　<フィルタ名>**

設定例　　**default_include telFIL**

解　説　　RADIUS認証において、RADIUS認証サーバから「.include」の拡張子があるFilter-Id attributeを指定されなかった場合には、このキーワードで指定したアクセスリスト（フィルタに一致したパケットを通過）が使用されるinterfaceに設定されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

RADIUS認証サーバから「.include」の拡張子があるFilter-Id attributeを指定された場合には、RADIUS認証サーバから受信したFilter-Id attributeが優先され、このキーワードで指定したフィルタは使用されません。

注　意　　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

default_exclude

キーワード **radiusファイル**

書　式　**default_exclude　<フィルタ名>**

設定例　**default_exclude telFIL**

解　説　RADIUS認証において、RADIUS認証サーバから「.exclude」の拡張子があるFilter-Id attributeを指定されなかった場合には、このキーワードで指定したアクセスリスト（フィルタに一致したパケットを廃棄）が使用されるinterfaceに設定されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

RADIUS認証サーバから「.exclude」の拡張子があるFilter-Id attributeを指定された場合には、RADIUS認証サーバから受信したFilter-Id attributeが優先され、このキーワードで指定したフィルタは使用されません。

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

default_outputfil

キーワード **radiusファイル**

書　式　**default_outputfil　<フィルタ名>**

設定例　**default_outputfil telFIL**

解　説　RADIUS認証において、RADIUS認証サーバから「.outputfil」の拡張子があるFilter-Id attributeが指定されなかった場合には、このキーワードで指定した出力フィルタが使用されるinterfaceに設定されます。
<フィルタ名>は、ipfiltersファイルで設定したフィルタ名を指定します。

RADIUS認証サーバから「.outputfil」の拡張子があるFilter-Id attributeを指定された場合には、RADIUS認証サーバから受信したFilter-Id attributeが優先され、このキーワードで指定したフィルタは使用されません。

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

clid_auth

キーワード **radiusファイル**

書　式　**clid_auth　{on｜off}**

デフォルト　**off**

解　説　ISDN着信時にRADIUS認証サーバを使用してCLID認証を行うかどうかを設定します。
「on」に設定すると、本装置のusersファイルに相手電話番号と一致するremote_tel/accept_telキーワードを含む%userエントリが見つからなかった場合に、RADIUS認証サーバを使用してCLID認証を行います。RADIUS認証サーバにおいて認証が成功した場合はISDNの着信を許可し、認証が失敗した場合はISDNの着信を拒否します。

設定なし、または「off」の設定の場合、本装置のusersファイルに相手電話番号と一致するremote_tel/accept_telキーワードを含む%userエントリが見つからなかった場合には、ISDNの着信を拒否します。

関　連　**本装置のusersファイルの%preset分類キーワードのclid_authキーワード**

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**
また、本装置のusersファイルの%preset 分類キーワードのclid_authキーワードの設定が「may」または「must」の場合にのみ有効です。

ext_passwd

キーワード **radiusファイル**

書　式　**ext_passwd　<パスワード>**

例　**ext_passwd radiuspasswd**

デフォルト　**siipassword**

解　説　ISDN着信時のCLID認証に使用するパスワードを設定します。
本装置は、ISDN着信時にCLID認証を行う場合、このキーワードで設定したパスワードを認証要求（AccessRequestパケット）のPassword attributeとしてRADIUS認証サーバに送信します。英数字で最大16文字です。

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

disconnect_cause

キーワード **radiusファイル**

書　式　**disconnect_cause　{on｜off}**

例　**disconnect_cause on**

デフォルト　**off**

解　説　RADIUSアカウントサーバに送信するAcct-Status-TypeがSTOPのアカウント要求（Accounting Request）パケットにAcct-Disconnect-Causeアトリビュートを入れるかどうかを設定します。
「on」に設定すると、Acct-Disconnect-Causeアトリビュートを入れてAcct-Status-TypeがSTOPのアカウント要求パケットを送信します。

注　意　**このキーワードは、%radius_auth分類キーワードのみに有効です。**

5.12　ippoolファイル

端末型接続において、本装置から接続相手にIPアドレスを割り当てる場合に、あらかじめ本装置にプールするIPアドレスを設定します。 RADIUS認証サーバを使用して認証を行う場合においても、IPプールからIPアドレスを割り当てる場合には、このippoolファイルに設定されたIPアドレスが使用されます。

書　式　**[%ippool　<プール番号>]**
<IPアドレス>[/<マスク>]　<個数>

例　1

172.31.1.1	**16**

例　2

172.31.1.1/24	**16**
172.31.1.100/24	**16**

例　3

%ippool	**1**	
	172.31.1.1/24	**16**
	172.31.1.100/24	**16**
%ippool	**2**	
	172.31.1.129/24	**16**

解　説　プールするIPアドレスを設定します。
本装置では、16個のIPプールを登録することが可能です。各IPプールはプール番号(1～16)で識別されます。プール番号は、%ippool分類キーワードの**<プール番号>**に、1～16の10進数で指定します。
%ippool分類キーワードの行を省略した場合、プール番号1のIPプールにプールされます。

プールされるアドレスは、**<IPアドレス>**で指定したIPアドレスから、**<個数>**で指定した数分のIPアドレスになります。
<IPアドレス>には、**<マスク>**でそのIPアドレスに対するマスクのビット長を、1～32の10進数で指定できます。<マスク>を省略した場合には、**<IPアドレス>**のクラスにしたがったマスクが設定されます。
各IPプールには、「**<IPアドレス>　<個数>**」を複数行設定できますが、プールできるIPアドレスの個数は、各プール毎に、最大512個です。

参　照　**「4章　4.4.7」**

5.13 serversファイル

ブート時に起動させる各種サーバプログラムを設定します。

書　式　　**<サーバプログラム名>　<パラメータ>**

例　　**/share/telnetd -CON**

解　説　　ブート時に起動させる各種サーバプログラムを設定します。
<パラメータ>は、サーバプログラムに渡す引き数です。
出荷時に本装置に起動させることが可能なサーバプログラムは、全て記述されています。サーバを起動する場合には、コメント「#」をはずしてください。また、サーバを起動させない場合には、コメント「#」を行の先頭に入れてください。

serversファイルのデフォルトの設定内容

```
#
/share/telnetd -CON          #TELNETサーバ
#
/share/vupd                  #VERSION UPサーバ
#
#/share/snmpd                #SNMPエージェント
#
#/share/routed               #RIP
```

5章 セットアップファイル・リファレンス

5.14　rip.confファイル

RIPの設定を行います。
rip.confファイルの変更内容はreloadコマンドを実行すると有効になります。

interface

キーワード　　**rip.confファイル**

書　式　　**interface　<論理インタフェース名>**

例　　**interface en0**

解　説　　RIPを使用する論理インタフェース名を指定します。

論理インタフェース名	説　　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
hsd∗	高速ディジタル回線の論理インタフェース名（∗：1〜）

指定しない論理インタフェースからRIPパケットを受信した場合は、そのパケットを廃棄します。

in

サブキーワード　　**rip.confファイル**

書　式　　**in　{rip1｜rip2｜both｜none}**

デフォルト　　**both**

例　　**in rip2**

解　説　　RIPパケット受信の制御方法を指定します。

rip1　：RIP1パケットのみを受信します。
rip2　：RIP2パケットのみを受信します。
both　：RIP1、RIP2の両方のパケットを受信します。
none　：RIPパケットを廃棄します。

out

サブキーワード **rip.confファイル**

書　式　**out　{rip1｜rip2｜rip2mcast｜none}**

デフォルト　**rip1**

例　**out rip2mcast**

解　説　RIPパケット送信の制御方法を指定します。

rip1	：	RIP1パケットをブロードキャストで送信します。
rip2	：	RIP2パケットをブロードキャストで送信します。
rip2mcast	：	RIP2パケットをマルチキャストで送信します。 マルチキャストアドレスは224.0.0.9です。
none	：	RIPパケットを送信しません。

auth

サブキーワード **rip.confファイル**

書　式　**auth　{passwd｜none}**

デフォルト　**none**

例　**auth passwd**

解　説　認証の使用を設定します。この設定はRIP2の場合に有効になります。

passwd	：	認証をシンプルパスワードで行います。 RIP1パケットと認証が成功したRIP2パケットを受け入れます。 RIP1パケットを廃棄したい場合には、受信の制御で「rip2」を指定してください。
none	：	認証を行いません。 RIP1パケットと認証のないRIP2パケットを受け入れます。 認証の付いたRIP2パケットは廃棄します。

passwd

サブキーワード **rip.confファイル**

書　式　**passwd　<パスワード>**

例　**passwd makuhari**

解　説　認証をシンプルパスワードで行う設定の場合にパスワードを設定します。パスワードは英数字で最大16文字です。

destination

キーワード **rip.confファイル**

書　式　**destination　<宛先アドレス>/<マスク>　[via　<経由ルータ>]　<メトリック>**

例　**destination 128.30.0.0/16 2**
destination 0.0/0 via 172.31.0.5 10

解　説　ISDN回線や高速ディジタル回線経由のルートやデフォルトルートなど、RIPで広告するルートを設定します。

<宛先アドレス>デスティネーションのネットワークアドレス、またはホストアドレスを設定します。

<マスク> **<宛先アドレス>**に対するマスクのビット長を10進数で設定します。デフォルトルートを設定する場合には、**<宛先アドレス>/<マスク>**を「0.0/0」と設定してください。

<経由ルータ> パケットをフォワーディングするルータの**<IPアドレス>**を指定します。ISDN経由のルートを広告する場合には、省略します。

<メトリック>このルートのメトリックを10進数で設定します。範囲は1から15です。

5.15 syslog.confファイル

本装置で発生したイベントを、syslogを使用してネットワーク上の他のホストへ通知するための設定を行います。syslogに出力されるメッセージの詳細は**「付録B　コンソールおよびsyslogに出力されるメッセージ一覧」**を参照してください。
syslog.confファイルの変更内容はreloadコマンドを実行すると有効になります。

mode

キーワード　　**syslog.confファイル**

書　式　　**mode　{on｜off}**

デフォルト　　**off**

例　　**mode on**

解　説　　syslogを使用するかどうかを指定します。
　　on　：syslogを使用する。
　　off　：syslogを使用しない。
「on」に設定した場合、hostキーワード、facilityキーワードの設定が必要になります。

host

キーワード　　**syslog.confファイル**

書　式　　**host　<送信先のホスト>**

例　1　　**host 172.16.1.3**
例　2　　**host hostA**

解　説　　syslogパケット送信先のホストを指定します。
ホスト名またはIPアドレスでの指定が可能です。

facility

キーワード **syslog.confファイル**

書　式　**facility　{local0｜local1｜local2｜local3｜local4｜local5｜local6｜local7}**

例　**facility local0**

解　説　syslogパケットにエンコードするファシリティを指定します。

srcaddr

キーワード **syslog.confファイル**

書　式　**srcaddr　{auto｜hostname｜specify　<IPアドレス>}**

デフォルト　**auto**

例　1　**srcaddr auto**
例　2　**srcaddr hostname**
例　3　**srcaddr specify 172.32.2.241**

解　説　本装置が送出するsyslogパケットの送信元IPアドレスの指定を行います。

auto　：送出インタフェースのIPアドレスを使います。
hostname　：自局ホスト名に対応するIPアドレスを使います。
specify　：<IPアドレス>で指定されたIPアドレスを使います。<IPアドレス>部分は、ホスト名での指定も可能です。

isdntrace

キーワード **syslog.confファイル**

書　式　**isdntrace　{on｜off}**

デフォルト　**off**

例　**isdntrace on**

解　説　ISDNカテゴリのトレースメッセージをsyslogで出力するかどうかを指定します。

on　：出力する。
off　：出力しない。

ppptrace

キーワード **syslog.confファイル**

書　式　**ppptrace　{on｜off}**

デフォルト　**off**

例　**ppptrace on**

解　説　PPPカテゴリのトレースメッセージをsyslogで出力するかどうかを指定します。
on　：出力する。
off　：出力しない。

sessiontrace

キーワード **syslog.confファイル**

書 式　**sessiontrace　{on｜off}**

デフォルト　**off**

例　**sessiontrace on**

解 説　SESSIONカテゴリのトレースメッセージをsyslogで出力するかどうかを指定します。
on　：出力する。
off　：出力しない。

radiustrace

キーワード **syslog.confファイル**

書　式　**radiustrace　{on｜off}**

デフォルト　**off**

例　**radiustrace on**

解　説　RADIUSカテゴリのトレースメッセージをsyslogで出力するかどうかを指定します。
on　：出力する。
off　：出力しない。

dsptrace

キーワード **syslog.confファイル**

書　式　**dsptrace　{on｜off}**

デフォルト　**off**

例　**dsptrace on**

解　説　DSPカテゴリのトレースメッセージをsyslogで出力するかどうかを指定します。

on　：出力する。
off　：出力しない。

5.16　servicesファイル

サービス名とポート番号の対応を設定します。

書　式　　**<サービス名>　<ポート番号>/<プロトコル名>　[<サービス別名>]**

例　　**ftp 21/tcp**

解　説　　サービス名と対応するポート番号を設定します。

<サービス名>	:	サービス名を指定します。
<ポート番号>	:	ポート番号を10進数で指定します。
<プロトコル名>	:	「tcp」または「udp」を指定します。
<サービス別名>	:	サービスの別名を指定します。

5.17　セットアップファイルの変更内容を有効にする方法

本装置のセットアップファイルを編集した場合、その変更内容を有効にする方法は、セットアップファイルによって異なります。**表5-7**にセットアップファイルの変更内容を有効にする方法をまとめて示します。

表5-7　セットアップファイルの変更内容を有効にする方法

ファイル名	変更内容を有効にする方法
hostname	再起動（rebootコマンド）
hosts	①hostnameファイルのホスト名に対する設定を変更する場合 再起動（rebootコマンド） ②他のセットアップファイルで参照しているホスト名に対する設定を変更する場合 そのセットアップファイルを有効にする方法 ③本装置からtelnetコマンドで指定するためのホスト名に対する設定を変更する場合 特に必要なし
boards	①ポートや論理チャネルの数を変更する場合、およびそのポートの回線種別を変更する場合 再起動（rebootコマンド） ②上記①以外の変更をする場合 reloadコマンド
interface	reloadコマンド
gateways	reloadコマンド
ipfilters	reloadコマンド
netmask	再起動（rebootコマンド）
resolv.conf	特に必要なし
snmpconf	snmprestartコマンド
users	reloadコマンド
radius	reloadコマンド
ippool	reloadコマンド
servers	再起動（rebootコマンド）
rip.conf	reloadコマンド
syslog.conf	reloadコマンド
services	①他のセットアップファイルで参照しているサービス名に対する設定を変更する場合 そのセットアップファイルを有効にする方法 ②本装置のサーバプログラムが参照しているサービス名に対する設定を変更をする場合 通常は再起動（rebootコマンド）

5.18　セットアップファイルの設定範囲とデフォルト値

(1) セットアップファイルの設定範囲とデフォルト値

本装置の各セットアップファイルにおいて、キーワードに設定範囲があるもの、キーワードのデフォルト値があるものについて、**表5-8**にまとめて示します。デフォルト値を持つキーワードをデフォルト値で使用する場合、そのキーワードは設定する必要はありません。

表5-8　設定値の範囲とデフォルト値

(1/2)

ファイル名	キーワード	設　定　範　囲	デフォルト値
gateways	<メトリック>	1～99	――
snmpconf	authenTrap	on／off	off
	linkTrap	on／off	off
boards	enable／disable	enable／disable	enable
	clid_require	on／off	off
users	idle_timeout	5～100000 （秒）	120
	idle_ctl	both／in／out	both
	session_timeout	5～100000 （秒）	3600
	auto_disconnect	on／off	on
	session_disconnect	on／off	off
	connect_on_demand	on／off	off
	accept_call	on／off	on
	clid_auth	must／may／off	off
	auth_request	none／pap／chap／either／ pap-／chap-／either-	none
	auth_accept	none／pap／chap／remote pap-／chap-／remote-	none
	protocol	ppp／mp／bacp	ppp
	multi_connect	on／off	off
	mp_port_min	1～8	1
	mp_port_max	1～8	2
	bod	on／off	on
	bod_ctl	out／in／both	out
	bod_add_rate	10～90 （%）	70
	bod_del_rate	10～90 （%）	30
	bod_sample_time	5～60 （秒）	15
	dns1	none／accept	none
	dns2	none／accept	none
	wins1	none／accept	none
	wins2	none／accept	none
	ippool	0～16	1
	cb	none／request／accept	none
	cb_type	cbcp／isdn	cbcp
	cb_mode	may／must	must

表5-8　設定値の範囲とデフォルト値

(2/2)

ファイル名	キーワード	設　定　範　囲	デフォルト値
radius	mode	on／off	off
	port		1645(%radius_auth) 1646(%radius_acct)
	timeout	1～255	3
	retry	1～255	10
	chkauth	on／off	on
	rtime	0～100000（秒）	0（ディセーブル）
	set_session_id	on／off	off
	base_session_id	dec／hex	hex
	stop_ignore	on／off	off
	clid_auth	on／off	off
	disconnect_cause	on／off	off
rip.conf	in	rip1／rip2／both／none	both
	out	rip1／rip2／rip2mcast／none	rip1
	auth	passwd／none	none
syslog.conf	mode	on／off	off
	facility	local0／local1／local2／local3／ local4／local5／local6／local7	——
	srcaddr	auto／hostname／specify <IPアドレス>	auto
	isdntrace	on／off	off
	ppptrace	on／off	off
	sessiontrace	on／off	off
	radiustrace	on／off	off
	dsptrace	on／off	off

(2) usersファイルに登録できる接続相手数について

本装置のusersファイルに登録できる接続相手数は最大512です。ただし以下の2つの制限事項がありますので、注意してください。

① 本装置のeditコマンドでusersファイルを編集する場合

本装置のeditコマンドで編集できる最大行数は、1500行です。したがってこの行数を越えて接続相手を登録することはできません。
editコマンドで編集できる行数を越えてしまった場合には、ホスト上で編集したusersファイルをloadコマンドで転送する方法があります。

② ホスト上で編集したusersファイルを、loadコマンドで本装置に転送する場合

本装置のセットアップファイルは、ワークステーションなどで編集した後でloadコマンドで本装置に転送することができます。（loadコマンドの使用方法は、**6章**のloadコマンドの項を参 照してください）
この場合には、usersファイルのサイズは900Kbytes以下であることが必要です。このサイズを越えた場合には、動作は保証されません。

多くの接続相手を登録する場合には、

- デフォルト値で使用する場合には、そのキーワードは設定しない。
- 多くの接続相手に共通な設定で%default分類キーワードに記述できるキーワードは、%default分類キーワードに記述し、設定の異なる接続相手のみ%user分類キーワードに設定する。

などにより、usersファイルの行数を少なくなるようにしてください。

なお、この最大登録数は、本装置のusersファイルに登録する接続相手のみですから、端末型接続でRADIUS認証サーバに設定した接続相手数は含まれません。

6章

コマンド・リファレンス

6章では、本装置の状態を表示させたり、セットアップファイルを確認するときなどに使用するコマンドについて説明しています。

本章の内容

6.1　コマンドの見方

本章では、コマンドをアルファベット順に次のように記載して説明しています。

コマンドの名称を示します。

show

機　　能　コマンドの機能を説明しています。

フォーマット　コマンドの入力フォーマットを示しています。
[　] でくくられたパラメータは省略することもできます。

パラメータ　パラメータの種類と機能を説明しています。

使　用　例　コマンドの使用例を示しています。

```
# show  hostname ↓
router_A
#
```

下線部が実際に入力するコマンドの部分です (ただし、下線は画面には表示されません)。
「↓」は、Returnキーを示します。

注　　意　コマンド使用上の注意事項を記述しています。

エ　ラ　ー　コマンド使用時のエラー発生時に表示されるエラーメッセージの内容と対処方法を説明しています。

解　　説　コマンドの説明の後、コマンドの機能や操作、および表示される内容について詳しく説明しています。

図6-1　コマンドの見方

6.2 コマンドの説明

使用できるコマンド一覧を**表6-1**に示し、以下に各コマンドについて説明します。

表6-1　コマンド一覧

コマンド名称	機　　能	一般ユーザ
auth	本装置にログインできるユーザの追加／削除／表示を行う	×
clear	セットアップファイルの内容を工場出荷時の状態に戻す	×
console	コンソール出力のオン／オフや、出力端末の切り替えを行う	×
date	日付および時刻の表示／設定を行う	△
disconnect	接続している回線を切断する	×
edit	セットアップファイルを編集する	×
help	コマンド一覧を表示する	○
ifstate	本装置の論理インタフェースのアップ、ダウンを行う	×
linestat	回線の状態または統計情報を表示する	○
lo	本装置からログアウトする	○
load	セットアップファイルのセーブ／リストアを行う	×
modemstat	ディジイタルモデムあるいはPIAFSで接続している回線の状態を表示する	○
mstat	本装置のメモリの使用状況を表示する	○
netstat	本装置のIPネットワークの状態や統計情報を表示する	○
page	コマンドの画面表示を画面単位に区切る	○
passwd	本装置にログインするためのパスワードを設定する	○
ping	IPネットワーク上の相手ホストとの通信の確認を行う	○
pstat	本装置のCPUの使用状況を表示する	○
radiusstat	RADIUS認証サーバおよびRADIUSアカウントサーバの状態を表示する	○
reboot	本装置をリブートする	×
reload	本装置のいくつかのセットアップファイルの変更内容を有効にする	×
ripstat	RIPの統計情報を表示します。	×
riptrace	受信したRIPパケットをコンソールに表示する	×
show	セットアップファイルの内容を表示する	×
shutdown	本装置をシャットダウンする	×
snmpreload	snmpconfファイルの変更内容を有効にする	×
snmprestart	SNMPを起動する	×
statclear	統計表示コマンドが表示する値をリセットする	×
su	スーパーユーザにログインする	○
telnet	telnetクライアントで相手ホストにログインする	○
traceroute	指定したホストに到達するためのルートを検査し、IPアドレスとパケットの往復時間の実測値を表示する	○
version	システムソフトウェアのバージョンを表示する	×
wanport	指定したPRIポートを一時的にenable／disable状態にする	×
write	設定したファイルをセットアップカードに保存する	×

○：使用可　×：使用不可　△：機能限定

auth

機　　能　本装置にログインできるユーザの追加／削除／表示を行います。

フォーマット

auth add ユーザ名　ユーザID
auth del ユーザ名
auth print

パラメータ

add	：ユーザを追加する
del	：ユーザを削除する
print	：ユーザを表示する
ユーザ名	：追加／削除するユーザ名
ユーザID	：ユーザ名に対応するユーザID（1～99）

使 用 例

ユーザを表示する

```
# auth print ↓
USER LIST
 name                 user ID
 admin                      0
 somebody                 100
#
```

ユーザ（ohtsuka）をユーザID=4で追加する

```
# auth add ohtsuka 4 ↓
#
```

ユーザ（ohtsuka）を削除する

```
# auth del ohtsuka ↓
#
```

注　　意　authコマンドで変更した内容をセットアップカードにセーブするにはwriteコマンドを実行してください。writeコマンドを実行しないで、リブートや電源をオフにすると変更内容が失われてしまいます。

clear

機　　能　セットアップファイルの内容を工場出荷時の状態に戻します。

フォーマット

clear ファイル名	指定されたファイルを工場出荷時の状態に戻す
clear -ip｜-wan｜-all	指定されたカテゴリのファイルをまとめて工場出荷時の状態に戻す

パラメータ

-ip	：	IPの設定に関連するファイル(hostname,hostsファイルを除く)を対象にする
-wan	：	WANの設定に関連するファイルを対象にする
-all	：	IP, WANに関連するファイルを対象にする

使 用 例

```
# clear -ip ↓
clear [services] ... OK.
clear [gateways] ... OK.
clear [resolv.conf] ... OK.
clear [netmask] ... OK.
clear [snmpconf] ... OK.
clear [ipfilters] ... OK.
clear [interface] ... OK.
#
```

注　　意　clearコマンドで変更した内容をセットアップカードにセーブするにはwriteコマンドを実行してください。writeコマンドを実行しないで、リブートや電源をオフにすると変更内容が失われてしまいます。

解　　説　　clearコマンドは、セットアップファイルを工場出荷時の状態に戻すコマンドです。
カテゴリごとに初期化されるファイル名は以下の通りです。

①-ip	：	services, gateways, resolv.conf, netmask, snmpconf, ipfilters, interface, rip.conf, syslog.conf
②-wan	：	boards, users, radius, ippool
③-all	：	-ip, -wanで対象となるファイル全て。

注　意　　**-ip, -allではhostnameファイルとhostsファイルおよびauthコマンドで設定した内容は、工場出荷時の状態には戻りません。**

console

機　　能　コンソール出力のオン / オフや、出力端末の切り替えを行います。

フォーマット

console　[-off]

console　-rev　文字数

パラメータ

-off	:	コンソール出力をオフにする
省略時	:	コンソール出力をオンにする
-rev	:	コンソールメッセージを再表示する
文字数	:	再表示する文字数

使 用 例

操作している端末にコンソール出力を開始する

```
# console ↓
#
```

コンソール出力を停止する

```
# console  -off ↓
#
```

コンソールメッセージを再表示する

```
# console  -rev  200 ↓
starting wan services.
starting net services.
telnetd: start listen[telnet]
#
```

注　　意　telnetで本装置にログインした端末にコンソール出力をしている場合には、telnetを終了してログアウトする前に必ずコンソール出力をオフにしてください。

解　説　consoleコマンドは、コンソール出力のオン/オフや、出力先を切り替えるコマンドです。

本装置は、回線の障害やセットアップの誤りなどのメッセージをコンソールに出力します。コンソールの出力先は、本装置のCONSOLEポートに接続した端末や、ネットワークからtelnetで本装置にログインした端末です。

コンソール出力がオフの状態でも、本装置の内部メモリに最新のコンソール出力がある程度保持されています。

(1) コンソール出力のオンと出力端末の切り替え

コンソール出力をオンにする場合には、出力したい端末で consoleコマンドを実行します。consoleコマンドの実行はすぐに終了して、プロンプトが表示され、コマンドを入力できる状態になります。

内部メモリにコンソール出力が保持されている場合には、保持されていたメッセージが表示されます。以降は、障害などが発生してコンソール出力が行われた時点で、この端末にメッセージが表示されます。

他の端末でコンソール出力がオンになっている状態で consoleコマンドを実行すると、コマンドを実行した端末にコンソール出力が切り替わります。

コンソール出力オンの設定

```
# console↓
#
```

(2) コンソール出力をオフにする

コンソール出力をオフにすると、端末へのコンソールメッセージの出力が停止します。コンソール出力がオフの状態でも、コンソールに出力されたメッセージは本装置内部のメモリにある程度は保持されます。

コンソール出力オフの設定

```
# console  -off↓
#
```

(3) コンソールメッセージを再表示する

すでに表示されたコンソールメッセージは、本装置の内部メモリにある程度保持されています。このメッセージを再表示することができます。
再表示を実行した端末が、その後のコンソールメッセージの出力先になります。

注 意　保持されているコンソールメッセージは、内部バッファのサイズを超えると新しいコンソールメッセージによって上書きされます。また、本装置の電源を切ったり、リブートした場合には、保持されていたメッセージは失われます。

コンソールメッセージを再表示する

```
# console  -rev  200↓
starting wan services.
starting net services.
telnetd: start listen[telnet]
#
```

date

機　　能　日付および時刻の表示 / 設定を行います。

フォーマット　date　[日付]

パラメータ　日付　：設定する日付と時刻 (年月日時分)
(日付および時刻を設定する)
省略時　：日付および時刻を表示する

使 用 例　日付および時刻を表示する

```
(1)ns>  date ↓
 Mon Jan 21 17:50:57 JST 2002
(1)ns>
```

日付および時刻を設定する（2002年1月7日16時44分）

```
# date  0201071644 ↓
#
```

解　　説　dateコマンドは、日付および時刻の表示 / 設定を行うコマンドです。

日付および時刻を設定する場合は、「年月日時分」の順で指定します。「年月日時分」はそれぞれ2桁で指定し、1桁のものには必ず前に0を付けて指定してください。
0201141130は、2002年1月14日11時30分を表します。

注　意　**一般ユーザは、日付および時刻の表示のみができます。**
設定することはできません。

disconnect

機　　能　現在接続しているISDN回線のBチャネルを切断します。

フォーマット

disconnect　ユーザ名
disconnect　-l　論理インタフェース名
disconnect　-l　all

パラメータ

ユーザ名　：接続している相手のユーザ名
論理インタフェース名　：linestatで表示される論理インタフェース名 (ncp#)

使　用　例

ユーザns192を切断する

```
# disconnect ns192
#
```

論理インタフェースncp1を切断する

```
# disconnect -l   ncp1
#
```

解　　説

disconnectコマンドは、現在接続されているISDNのBチャネルを切断するためのコマンドです。切断する接続相手は、ユーザ名あるいは論理インタフェース名で指定します。
disconnectコマンドを使用する場合、linestatコマンドを実行すると、切断したい相手のユーザ名、あるいは論理インタフェース名がわかります。「linestat」と入力すると、以下のように表示されます。

```
# linestat ↓
Fri Mar 16 21:25:46 JST 2001
<PPP status>
 INTERFACE   STATE      PROTOCOL  PORT    CH    CONNECT-TIME     USER-NAME
 ncp1        connect     PPP       1-1    B1    03/16 21:24:43  ns192
```

ユーザ名は、右端の「USER-NAME」の部分に表示されています。また論理インタフェース名は、左端の「INTERFACE」の部分に表示されています。

6章　コマンド・リファレンス

したがってユーザns192をユーザ名を指定して切断したい場合には、次のように入力します。

```
# disconnect  ns192
#
```

またこのユーザns192を論理インタフェース名を指定して切断したい場合には、次のように入力します。

```
# disconnect  -l  ncp1
#
```

コマンドの実行結果は、再度linestatコマンドを実行することによって確認することができます。

注　意　**disconnectコマンドは、現在接続状態にある接続相手（linestatコマンドで、STATEの部分が「CONNECT」になっている接続相手）のみ有効です。**

edit

機　　能　セットアップファイルの編集を行います。

フォーマット　edit　ファイル名

edit　-h

パラメータ

ファイル名	:	編集するファイル名
-h	:	ファイル名の一覧を表示する

使 用 例　ファイルを編集する

```
# edit  hosts ↓
0001 # Internet Hostname file
```

解　　説　editコマンドの詳細な使用法は、「**付録A　エディタの使い方**」を参照してください。

help

機　　能　コマンド一覧を表示します。

フォーマット　help

パラメータ　なし

使 用 例　コマンド一覧を表示する

```
#help ↓
auth         add/delete/print user
clear        clear setup files to default
console      switch on/off console message
date         print/set date
        :
        :
write        write setup files to setup card
#
```

ifstate

機　　能　本装置の論理インタフェースのアップ、ダウンを行います。

フォーマット　ifstate　論理インタフェース名　up ｜ down

パラメータ

論理インタフェース名	：	アップ、ダウンを行う論理インタフェース名
up	：	指定した論理インタフェースをアップにする。
down	：	指定した論理インタフェースをダウンにする。

使 用 例　論理インタフェースen0をダウンにする

```
# ifstate en0 down ↓
#
```

解　　説　ifstateコマンドは本装置の論理インタフェースの状態をアップ、ダウンさせるコマンドです。
状態を変更することが可能な論理インタフェース名は以下のとおりです。

論理インタフェース名	説　　明
en0	LAN1ポートの論理インタフェース名
en1	LAN2ポートの論理インタフェース名
hsd*	高速ディジタル回線の論理インタフェース名（*：1～）

注　意　**論理インタフェースの状態が変更されたことを確認するには、「netstat -i」コマンドを実行してください。**

linestat

機　能　回線の状態または統計情報を表示します。

フォーマット

linestat [-s]

linestat isdn [-s | -s2]

linestat -P

パラメータ

省略時	：	PPPの状態を表示する
-s	：	LANとPPPの統計情報を表示する
isdn	：	ISDNの回線状態を表示する
isdn -s	：	ISDNの統計情報を表示する
isdn -s2	：	ISDNの回線サービスごとの統計情報を表示する
-P	：	LANとPRIのレイヤ1、ISDNのDチャネルのレイヤ2の状態を表示する

使用例　PPPの状態を表示する

```
(1)ns> linestat ↓
Fri Mar 16 21:25:46 JST 2001
<PPP over ISDN status>
 INTERFACE  STATE      PROTOCOL  PORT  CH   CONNECT-TIME    USER-NAME
 ncp1       connect    PPP        1-1  B1   03/16 21:24:43  ns192-1
```

ISDNの統計情報を表示する

```
(1)ns> linestat isdn -s ↓
Fri Mar 16 21:26:00 JST 2001
<ISDN statistics>
  PORT   IN-CALL     IN-CONNECT     OUT-CALL     OUT-CONNECT    CHARGE
   1-1         0              0            1               1        10
```

解　説　linestatコマンドは、現在の回線の状態または統計情報を表示するコマンドです。指定するパラメータによって、表示される内容は異なります。

(1) PPPの状態の表示

現在のPPPの接続の状態をISDN回線および高速ディジタル回線の論理インタフェースごとに表示します。なお、ステートがdisconnectの場合は表示されません。

```
(1)ns> linestat ↓
Fri Mar 16 21:25:46 JST 2001 ――― 時刻
<PPP over ISDN status>
 INTERFACE  STATE     PROTOCOL PORT  CH   CONNECT-TIME   USER-NAME
 ncp1       connect   PPP       1-1  B1   03/16 21:24:43 ns192-1
 ncp10      connect   MP        1-2  B11  02/28 10:11:13 siins
<PPP over HSD status>
 INTERFACE  STATE     PROTOCOL PORT  CH   CONNECT-TIME   USER-NAME
 hsd1       connect   PPP       1-5   1   01/04 09:10:58
 hsd10      connect   PPP       1-6  10   02/01 20:30:01
```

論理インタフェース名　ステート　プロトコル　拡張ボードスロット番号 - ポート番号　チャネル番号　接続時刻　接続相手名

時刻
：現在の時刻が表示されます。

論理インタフェース名
：ISDN回線および高速ディジタル回線の論理インタフェース名が表示されます。
ISDN回線の論理インタフェース名は「ncp∗」と表示されます。
高速ディジタル回線の論理インタフェース名は「hsd∗」と表示されます。

ステート
：現在のステートが表示されます。

connecting　：接続要求状態
connect　：接続確立状態
disconnecting：切断要求状態

プロトコル
：ステートがconnectの場合、使用しているPPPのプロトコルが表示されます。

PPP　：PPP（Point-to-Point Protocol）
MP　：MP（Multi-Link Protocol）
BACP：BACP（Band width Allocation control Protocol）

拡張ボードスロット番号 - ポート番号

：ステートがconnectの場合、使用している拡張ボードのスロット番号とPRIポートのポート番号が表示されます。

チャネル番号

：ステートがconnectの場合、ISDN回線であれば使用しているBチャネル番号が表示され、高速ディジタル回線であればboardsファイルの%channelで設定した論理チャネル番号が表示されます。

接続時刻

：ステートがconnectの場合、接続が確立した時刻が表示されます。

接続相手名

：接続相手のユーザ名が表示されます。PPP認証を使用している場合には、PPP認証で使用される相手のユーザ名が表示されます。PPP認証を使用せずにCLID認証のみで接続している場合には、その接続相手の電話番号（例：相手の電話番号が、03-5555-6666の場合「0355556666」）が表示されます。

(2) LANとPPPの統計情報の表示

LANとPPPの送信／受信のパケット数の統計情報を論理インタフェースごとに表示します。この統計情報は、各論理インタフェースごとの情報です。PPPの接続の場合、本装置では、論理インタフェースと接続相手は固定的には対応していませんので、各論理インタフェースの情報には複数の接続相手の統計が加算されています。

```
(1)ns> linestat -s ↓
Fri Mar 16 21:25:50 JST 2001
<LAN over ISDN statistics>
 NAME  INPUT(U) OUTPUT(U) INPUT(M) OUTPUT(M) IBUSY  OBUSY  IERR OERR
  en0        0         0       11         0      0      0     0    0
  en1       14        21        1         2      0      0     0    0

<PPP over ISDN statisics>
           [    Total Info.    ]  [ CurrentCall Info. ]
 INTERFACE IN-PACKET  OUT-PACKET  IN-PACKET  OUT-PACKET  USER-NAME
 ncp1           2266        1331         23          18   userA
 ncp2           5980        4727

<PPP over HSD statistics>
           [    Total Info.    ]  [ CurrentCall Info. ]
 INTERFACE IN-PACKET  OUT-PACKET  IN-PACKET  OUT-PACKET  USER-NAME
 hsd1        1195506      201099    1195506      201099
 hsd2        1195557      201109    1195557      201109
```

LANの統計情報
時刻
論理インタフェース名
入力ユニキャストパケット数
出力ユニキャストパケット数
入力マルチキャストパケット数
出力マルチキャストパケット数
入力ビジー数
出力ビジー数
入力エラー数
出力エラー数
現在接続中の呼についての接続相手名
PPPの統計情報
論理インタフェース名
入力パケット数
出力パケット数
現在接続中の呼についての入力パケット数
現在接続中の呼についての出力パケット数

時刻

：現在の時刻が表示されます。

LANの統計情報

論理インタフェース名

：論理インタフェース名が表示されます。

入力ユニキャストパケット数
：受信したユニキャストパケットの数が表示されます。

出力ユニキャストパケット数
：送信したユニキャストパケットの数が表示されます。

入力マルチキャストパケット数
：受信したマルチキャストパケットの数が表示されます。

出力マルチキャストパケット数
：送信したマルチキャストパケットの数が表示されます。

入力ビジー数
：受信ビジーの数が表示されます。

出力ビジー数
：送信ビジーの数が表示されます。

入力エラー数
：受信エラーの数が表示されます。

出力エラー数
：送信エラーの数が表示されます。

PPPの統計情報

論理インタフェース名
：論理インタフェース名が表示されます。

入力パケット数
：受信したデータパケット数が表示されます。

出力パケット数
：送信したデータパケット数が表示されます。

現在接続中の呼についての入力パケット数
：現在接続中の呼について、受信したデータパケット数が表示されます。
なお、呼が接続されていない場合、このカラムには何も表示されません。

現在接続中の呼についての出力パケット数
：現在接続中の呼について、送信したデータパケット数が表示されます。
なお、呼が接続されていない場合、このカラムには何も表示されません。

現在接続中の接続相手名

：現在接続中の接続相手のユーザ名が表示されます。
なお、呼が接続されていない場合、このカラムには何も表示されません。

(3) ISDNの回線状態の表示

ISDNの回線の状態を各Bチャネルごとに表示します。

```
(1)ns> linestat isdn ↓
Fri Mar 16 21:25:55 JST 2001
<ISDN status>
 PORT   CH  STATE                 TYPE     CONNECT-TIME    TELNO
  1-1   B1  enable :connect(Out) HDLC     03/16 21:24:42  0474706014*236
  1-1   B2  enable :disconnect
```

時刻　チャネル番号　ステート　回線サービス　接続時刻　相手電話番号
拡張ボードスロット番号 - ポート番号

時刻

：現在の時刻が表示されます。

拡張ボードスロット番号 - ポート番号

：拡張ボードのスロット番号とPRIポートのポート番号が表示されます。

チャネル番号

：Bチャネル番号が表示されます。

ステート

：そのチャネル番号の現在のステートが表示されます。ステートは「情報1：情報2」の形式で表示されます。

情報1は、boardsファイルのenable／disableの設定内容が表示され、表示内容は以下のとおりです。

enable	：enable状態（そのチャネルは使用可能である）
disable	：disable状態（そのチャネルは使用禁止である）

情報2は、そのチャネルの現在の状態が表示され、表示内容は以下のとおりです。

connecting	：発信中
connected	：着信中
connect(In)	：接続状態（着信で接続）
connect(Out)	：接続状態（発信で接続）
disconnect	：非接続状態
disconnecting	：切断中

なお、情報2が「接続状態」で、そのポートに対するboardsファイルの設定をenableからdisableに変更した場合、「disable:connect(In)」のように表示されます。
この場合現在の接続が終了した後（非接続状態になった後）、そのポートは使用禁止になります。

回線サービス

：ステートがconnectの場合、現在使用している回線サービスが表示されます。

HDLC	：回線交換でHDLCフレームで接続
PIAFS	：回線交換でPIAFS（V1.0）で接続
PIAFS20	：回線交換でPIAFS（V2.0）で接続
PIAFS21	：回線交換でPIAFS（V2.1）で接続
MODEM	：回線交換でMODEMで接続

接続時刻

：ステートがconnectの場合、接続が確立した時間が表示されます。

相手電話番号

：接続相手の電話番号が表示されます。ただし、着信時に網から発信者番号が通知されなかった場合は表示されません。

(4) ISDNの統計情報の表示

ISDNの回線使用に関する統計情報をポートごとに表示します。

```
(1)ns> linestat isdn -s ↓
Fri Mar 16 21:26:00 JST 2001 ──── 時刻
<ISDN statistics>
   PORT  IN-CALL  IN-CONNECT   OUT-CALL   OUT-CONNECT   CHARGE
    1-1       23          20         10            10      160
```

着信トータル回数　**着信接続回数**　**発信トータル回数**　**発信接続回数**　**課金情報**

拡張ボードスロット番号 - ポート番号

時刻

：現在の時刻が表示されます。

拡張ボードスロット番号 - ポート番号

：拡張ボードのスロット番号とPRIポートのポート番号が表示されます。

着信トータル回数

：そのポートにISDNで着信したトータル回数が表示されます。

着信接続回数

：そのポートにISDNで着信し、接続した（着信を許可した）回数が表示されます。

発信トータル回数

：そのポートからISDNで発信したトータル回数が表示されます。

発信接続回数

：そのポートからISDNで発信し、接続した（発信が成功した）回数が表示されます。

課金情報

：そのポートからISDNで接続し、切断時にISDN交換機から通知された課金情報のトータルが表示されます。単位は円です。

また、-sでなく-s2を指定することで、回線サービスごとに分けて表示することもできます。

```
(1)ns> linestat isdn -s2 ↓
Fri Mar 16 21:26:00 JST 2001
<ISDN statistics>
  PORT   IN-CALL  IN-CONNECT   OUT-CALL  OUT-CONNECT   CHARGE
   1-1
  HDLC        11          11         11           10      160
  PIAFS        2           1          0            0        0
  MODEM       10           8          0            0        0
  TOTAL       23          20         10           10      160
```

分類

分類

：どの回線サービスに関する統計情報であるかを示します。

HDLC	：回線サービスがHDLCの呼に関する統計
PIAFS	：回線サービスがPIAFSの呼に関する統計
MODEM	：回線サービスがMODEMの呼に関する統計
TOTAL	：すべての回線サービスを合計した統計

(5) LANとPRIのレイヤ1、ISDNのDチャネルのレイヤ2の状態の表示

現在のLANポートのレイヤ1の状態とPRIポートのレイヤ1の状態、およびISDNのDチャネルのレイヤ2（LAPD）の状態が表示されます。

```
(1)ns> linestat -P ↓
Fri Mar 16 21:26:00 JST 2001 ―――――――――― 時刻
<LAN layer1 status>
   en0             layer1:LINK-OK REMOTE-OK   100M-FULL
   en1             layer1:LINK-OK REMOTE-OK   100M-FULL
論理インタフェース名      レイヤ1ステート          LANのレイヤ1の状態

<PRI layer1/layer2 status>
   1-1        layer1:F1(RUNNING) layer2:ESTABLISH      (TEI:0)
   1-6        layer1:F1(RUNNING)
```

レイヤ1ステート　レイヤ2ステート　TEI値

拡張ボードスロット番号 - ポート番号　PRIのレイヤ1／レイヤ2の状態

時刻

：現在の時刻が表示されます。

LANのレイヤ1の状態

論理インタフェース名

：論理インタフェース名が表示されます。

レイヤ1ステート

：LANポート（論理インタフェース）の現在のレイヤ1の状態が表示されます。

LINK-NG	：リンクが確立していない状態
LINK-OK	：リンクが確立している状態
REMTOE-NG	：リモートフォルトを検出した状態（リンクが確立している状態で有効）
REMOTE-OK	：リモートフォルトを検出していない状態（リンクが確立している状態で有効）
100M-FULL	：100M全二重（リンクが確立している状態で有効）
100M-HALF	：100M半二重（リンクが確立している状態で有効）
10M-FULL	：10M全二重（リンクが確立している状態で有効）
10M-HALF	：10M半二重（リンクが確立している状態で有効）

PRIのレイヤ1／レイヤ2の状態

拡張ボードスロット番号 - ポート番号

：拡張ボードのスロット番号とPRIポートのポート番号が表示されます。

レイヤ1ステート

：PRIポートの現在のレイヤ1の状態が表示されます。

F0(POWER OFF)	：信号の送受信ができない状態
F1(RUNNING)	：レイヤ1の同期が確立している状態
F2(RX_RAI)	：障害状態1の状態
F3(LOST_SIG)	：障害状態2の状態
F4(RX_AIS)	：障害状態3の状態
F5(CRC_ERR)	：障害状態4の状態

レイヤ2ステート

：PRIポートの現在のISDNのDチャネルレイヤ2（LAPD）の状態が表示されます。高速ディジタル回線の場合は表示されません。

NULL	：非接続状態（TEI値なし）
TEI	：非接続状態（TEI値割当て）
AWAIT_EST	：接続要求状態
ESTABLISH	：接続確立状態

TEI値

：PRIポートのISDNのDチャネルレイヤ2（LAPD）で使用しているTEI値が表示されます。高速ディジタル回線の場合は表示されません。

lo

機　　能　本装置からログアウトします。

フォーマット　lo

パラメータ　なし

使 用 例　本装置からログアウトする

```
(1)ns> lo↓
login:
```

load

機　　能　セットアップファイルのセーブ / リストアを行います。

フォーマット　load［-s　ソースIPアドレス］ホスト名

パラメータ

ソースIPアドレス　：パケットのソースIPアドレス。省略時は自局ホスト名に対応したIPアドレスになります。自局IPアドレスのいずれかである必要があります。

ホスト名　：セーブ / リストアを行うホスト名

使　用　例

すべてのセットアップファイルをホスト「host1」のディレクトリ「ns1.setup」にセーブする。

```
# load  host1 ↓
login: user1 ↓
passwd:_________↓
load> storea  ns1.setup ↓
store file [ns1.setup/hosts].
store file [ns1.setup/services].
       ・
       ・
       ・
load> quit ↓
#
```

全てのセットアップファイルをホスト「host1」のディレクトリ「ns1.setup」からリストアする。

```
# load  host1↓
login: user1↓
passwd:_______↓
load> loada  ns1.setup↓
load file [ns1.setup/hosts].
load file [ns1.setup/services].
         ・
         ・
         ・
load> quit↓
#
```

注　　意

- すべてのセットアップファイルをセーブするには、ホスト上に900kByte以上の空き領域が必要です。
- ftpサーバをサポートしているホストが必要です。
- loadコマンドでリストアした内容をセットアップカードにセーブするには、writeコマンドを実行してください。writeコマンドを実行しないで、リブートや電源をオフにすると変更内容が失われてしまいます。

エ　ラ　ー

エラーメッセージ	意　味	対　処
Connect error	コネクションの開設に失敗した	指定したホストが立ち上がっているか、ネットワークケーブルが正しく接続されているかを確認してください。 相手のホストでFTPサーバが立ち上がっているか確認してください。 指定したホスト名が正しいか確認してください。 gatewaysファイルの設定が正しいか確認してください。
unknown host	指定したホスト名が見つからない	①指定したホスト名が正しいか、hostsファイルに登録されているかを確認してください。 ②ドメインネームシステムを使用している場合には、ドメインサーバ上のホスト名の登録を確認してください。
Login inconnect	ログインに失敗した	指定したユーザ名、パスワードを確認してください。

解　　説　loadコマンドは、ftpプロトコルを利用して本装置のセットアップファイルをホストにセーブ / リストアするコマンドです。本装置はftpのクライアントとして動作し、ホストのftpサーバとファイルの転送を行います。

(1) ホストへのログイン

loadコマンドを起動して、ftpでホストにログインします。プロンプト「login:」に対してユーザ名を入力し、プロンプト「passwd:」に対してそのユーザのパスワードを入力します。ホストへのログインが成功するとプロンプト「load>」が表示され、loadコマンドのサブコマンドが入力できる状態になります。

ホストへのログイン

```
# load  host1 ↓
login:  user1 ↓
passwd: ________↓
load>
```

サブコマンド一覧

サブコマンド	意　　味
cd	ディレクトリを移動する
loada	すべてのセットアップファイルをリストアする
storea	すべてのセットアップファイルをセーブする
load	指定したセットアップファイルをリストアする
store	指定したセットアップファイルをセーブする
ls	ディレクトリの内容を出力する
quit	コマンドを終了する

(2) ディレクトリの移動

ホスト上の作業ディレクトリを指定したディレクトリに移動します。

```
load> cd ns1.setup ↓          移動するホスト上のディレクトリ名
```

(3) すべてのセットアップファイルのセーブ／リストア

すべてのセットアップファイルをホスト上の指定したディレクトリにセーブ / リストアします。

```
load> storea ns1.setup ↓      セーブするディレクトリ名
または
load> cd ns1.setup ↓          移動するホスト上のディレクトリ名
load> storea ↓
```

```
load> loada ns2.setup ↓          リストアするディレクトリ名
または
load> cd ns2.setup ↓             移動するホスト上のディレクトリ名
load> loada ↓
```

注 意　　authコマンドで設定した内容は、セーブ/リストアされません。

(4) 指定したセットアップファイルのセーブ / リストア

指定したセットアップファイルをホスト上にセーブ / リストアします。

```
load> store gateways ↓           セーブするファイル名
```

```
load> load users ↓               リストアするファイル名
```

(5) ホスト上のディレクトリの内容の出力

ホスト上のディレクトリの内容を要約した形式で出力します。ディレクトリ名を省略するとホスト上のカレントディレクトリの内容が出力されます。

```
load> ls ns1.setup ↓             ホスト上のディレクトリ名
または
load> cd ns1.setup ↓             移動するホスト上のディレクトリ名
load> ls ↓
```

(6) loadコマンドの終了

loadコマンドを終了します。

```
load> quit ↓
#
```

modemstat

機　　能　ディジタルモデムあるいはPIAFSで接続している回線の詳細な状態を表示します。

フォーマット　modemstat

パラメータ　なし

使 用 例

```
Fri Mar 16 11:54:08 JST 2001
<DigitalModem & Piafs status>
No  PORT  CH  STATE       CARRIER  R-RATE T-RATE  PROTOCOL COMP
1    1-1  B1  CONN        V34      31200  33600   LAPM     V42BIS
2    1-1  B2  CONN        PIAFS    64000  64000   PIAFS20  NONE
3    1-1  B3  CONN        PIAFS    64000  32000   PIAFS21  NONE
4    1-1  B4  CONNECTING  -----    -----  -----   -------  ----
     ---  --  ----------  -----    -----  -----   -------  ----
```

解　　説　modemstatコマンドは、NS-421-10/30 DSP拡張ボードを使用している場合に、ディジタルモデム、あるいはPIAFSで接続している回線の詳細な状態を表示するコマンドです。

```
Fri Mar 16 11:54:08 JST 2001 ─────────────── 時刻
<DigitalModem & Piafs status>
No  PORT  CH  STATE       CARRIER  R-RATE T-RATE  PROTOCOL COMP
1    1-1  B1  CONN        V34      31200  33600   LAPM     V42BIS
2    1-1  B2  CONN        PIAFS    64000  64000   PIAFS20  NONE
3    1-1  B3  CONN        PIAFS    64000  32000   PIAFS21  NONE
4    1-1  B4  CONNECTING  -----    -----  -----   -------  ----
     ---  --  ----------  -----    -----  -----   -------  ----
```

番号　拡張ボードスロット番号 - ポート番号　チャネル番号　ステート　通信規格　受信速度　送信速度　プロトコル　圧縮方式

ポート番号、チャネル番号、ステート、通信規格、受信速度、送信速度、プロトコル、圧縮方式は、現在ディジタルモデムあるいはPIAFSで使用されていない場合、あるいはまだ確定していない場合には、「-----」と表示されます。

番号

：装置内部で管理している番号が表示されます。

時刻

：現在の時刻が表示されます。

拡張ボードスロット番号 - ポート番号

：拡張ボードのスロット番号とPRIポートのポート番号が表示されます。

チャネル番号

：使用しているBチャネル番号が表示されます。

ステート

：そのチャネルがディジタルモデムあるいはPIAFSで使用されている場合、現在のステートが表示されます。

CONNECTING	：接続処理中
CONN	：接続状態
DISCONNECT	：切断処理中

通信規格

：ディジタルモデムの相手モデムと接続した時には、選択されたモデムの通信規格が表示されます。

V90	：V.90
K56F	：K56flex
V34	：V.34
V32BIS	：V.32bis
V32	：V.32

PIAFSで相手装置と接続している場合には、「PIAFS」と表示されます。

受信速度

：ディジタルモデムの相手モデムと接続した時には、選択された受信速度が単位bpsで表示されます。ただしこの速度は、回線の状況に応じて相手モデムとの間でネゴシエーションが行われて、変化している可能性があります。PIAFSで相手装置と接続している場合には、以下のように表示されます。

32000 ：PIAFSのV1.0の装置と接続している場合

64000 ：PIAFSのV2.0あるいはV2.1の装置と接続している場合

送信速度

：ディジタルモデムの相手モデムと接続した時には、選択された受信速度が単位bpsで表示されます。ただしこの速度は、回線の状況に応じて相手モデムとの間でネゴシエーションが行われて、変化している可能性があります。また受信速度と送信速度が同じ速度である通信規格の場合、「-----」と表示されます。

PIAFSで相手装置と接続している場合には、現在の接続速度が以下のように表示されます。

32000　：PIAFSのV1.0の装置と接続している場合、およびPIAFSのV2.1の装置と接続していて、現在32Kbpsで接続している場合。

64000　：PIAFSのV2.0の装置と接続している場合、およびPIAFSのV2.1の装置と接続していて、現在64Kbpsで接続している場合。

プロトコル

：ディジタルモデムの相手モデムと接続した時には、選択されたモデム通信のデータプロトコルが表示されます。

LAPM　：LAPM (V.42)

MNP　：MNP

PIAFSで相手装置と接続している場合には、使用しているPIAFSのプロトコルバージョンが以下のように表示されます。

PIAFS10　：PIAFSのV1.0（32Kbps固定）で接続

PIAFS20　：PIAFSのV2.0（64Kbps固定）で接続

PIAFS21　：PIAFSのV2.1（64Kbps／32Kbps速度可変）で接続

圧縮方式

：ディジタルモデムの相手モデムと接続した時には、選択されたモデム通信の圧縮方式が表示されます。

V42BIS　：V.42bis

MNP5　：MNP5

PIAFSで相手装置と接続している場合には、「NONE」と表示されます。

mstat

機　　能　本装置のメモリの使用状況を表示します。

フォーマット　mstat

パラメータ　なし

使 用 例　メモリの使用状況を表示する

```
(1)ns> mstat ↓
Core     28% utilized.
Buffer   13% utilized.
(1)ns>
```

解　　説　mstatコマンドは本装置のメモリの使用状況を表示するコマンドです。
本装置のシステムが使用するエリアと通信用のバッファエリアの使用状況をパーセントで確認できます。

メモリの使用状況を表示する

```
(1)ns> mstat ↓
Core     28% utilized. ――――― システムエリア使用率
Buffer   13% utilized. ――――― バッファエリア使用率
(1)ns>
```

システムエリア使用率

：本装置のシステムソフトウェアが使用するメモリエリアの使用率をパーセントで表示します。

バッファエリア使用率

：本装置が受信データや送信データを格納するバッファエリアの使用率をパーセントで表示します。

netstat

機　　能　本装置のIPネットワークのインタフェースの状態や統計情報およびルーティング情報を表示します。

フォーマット　netstat　[-n] [-r | -i | -ip | -tcp | -tcpp | -udp | -udpp | -fil]

パラメータ

省略時	：	TCPコネクションの状態を表示する
-n	：	IPアドレスをホスト名で表示する
-r	：	現在のルーティング情報を表示する
-i	：	IPインタフェースの状態を表示する
-ip	：	IPの統計情報を表示する
-tcp	：	TCPの統計情報を表示する
-tcpp	：	TCPのコネクションの状態を表示する
-udp	：	UDPの統計情報を表示する
-udpp	：	UDPの状態を表示する
-fil	：	アクセスリストおよびアウトプットフィルタの統計情報を表示する

使　用　例　TCPのコネクションの状態を表示する

```
(1)ns> netstat ↓
 TCP CONNECTION STATUS
  LISTEN        <x  0,r  0> (0.0.0.0).23 <—> (0.0.0.0).0
  ESTABLISHED   <x  0,r  0> (128.30.2.41).23 <—> (128.30.0.122).1248
(1)ns>
```

現在のルーティング情報を表示する

```
(1)ns> netstat -r ↓
ROUTING TABLE
 destination    mask        gateway      if      property           cost
*130.30.0.0     ffff0000    130.30.0.1   ncp1    -----                 1
*130.30.0.1     ffffffff                 ncp1    -----                 -
 129.30.0.0     ffff0000    128.30.2.50  en0     -----                 1
 128.30.0.0     ffff0000                 en0     direct                -
 0.0.0.0        00000000                 ipnhr0  direct                -
 127.0.0.2      ffffffff                 sink0   p-to-p,unnumbered     -
 128.30.2.41    ffffffff                 lo0     p-to-p,loop           -
 127.0.0.1      ffffffff                 lo0     p-to-p,loop           -
(1)ns>
```

IPインタフェースの状態を表示する

```
(1)ns> netstat -i ↓
 INTERFACE STATUS
 name    desired-state    op-state       mtu    address        class
 lo0                UP          UP      1024    127.0.0.1      -----
 sink0              UP          UP      1024    -----          -----
 ipnhr0           DOWN        DOWN     32000    -----          -----
 en0                UP          UP      1500    128.30.2.41    -----
 ncp1               UP          UP      1500    130.30.0.1     -----
(1)ns>
```

TCPの統計情報を表示する

```
(1)ns> netstat -tcp ↓
TCP STATISTICS
       active open          1
       passive open         0
       input seg           29
       input error          0
       retransmit           0
       output seg         592
       output reset         1
(1)ns>
```

解　　説　netstatコマンドはIPのルーティング情報およびIPインタフェース(論理インタフェース)の状態や統計情報 を表示するコマンドです。
また、本装置が立ち上がってからのTCP、UDP、IPの統計情報を表示したり、本装置のTCPのコネクションの状態やUDPの状態を確認することができます。

(1) IPのルーティング情報を表示する

現在のルーティング情報の表示例

```
(1)ns> netstat -r ↓
 ROUTING TABLE
 destination  mask      gateway      if      property          cost
*130.30.0.0   ffff0000  130.30.0.1   ncp1    -----                1
*130.30.0.1   ffffffff               ncp1    -----                -
 133.30.0.1   ffffffff               hsd1    p-to-p               -
 129.30.0.0   ffff0000  128.30.2.50  en0     -----                1
 128.30.0.0   ffff0000               en0     direct               -
 0.0.0.0      00000000               ipnhr0  direct               -
 127.0.0.2    ffffffff               sink0   p-to-p,unnumbered    -
 128.30.2.41  ffffffff               lo0     p-to-p,loop          -
 127.0.0.1    ffffffff               lo0     p-to-p,loop          -
*192.168.1.0  ffffff00  128.30.0.100 en0     RIP                  5
(1)ns>
```

デスティネーション　**ネットマスク**　**ゲートウェイ**　**インタフェース**　**属性**　**コスト**

デスティネーション
：宛先のネットワークやホストのアドレスが表示されます。

ネットマスク
：デスティネーションのネットマスクが表示されます。

ゲートウェイ
：次ホップのルータのIPアドレスが表示されます。

インタフェース
：論理インタフェース名が表示されます。

属性
：インタフェースやルートの属性が表示されます。

direct　：直接接続ネットワーク
p-to-p　：ポイント・ツー・ポイント
RIP　　：ルーティングプロトコルとしてRIPを使用

コスト
：コスト値が表示されます。

注 意　**usersファイルで指定したルーティング情報は、回線接続中のみ先頭に「＊」が付いて表示されます。**
また、RIPにより取得したルーティング情報にも、先頭に「＊」が付いて表示されます。

(2) IPインタフェースの状態を表示する

IPインタフェースの状態の表示例

```
(1)ns> netstat  -i ↓
INTERFACE STATUS
 name    desired-state   op-state     mtu   address       class
 lo0                UP         UP    1024   127.0.0.1     -----
 sink0              UP         UP    1024   -----         -----
 ipnhr0           DOWN       DOWN   32000   -----         -----
 en0                UP         UP    1500   128.30.2.41   -----
 hsd1               UP         UP    1500   133.30.0.1    -----
 ncp1               UP         UP    1500   130.30.0.1    -----
(1)ns>
```

インタフェース　要求ステート　現在ステート　最大送信長　アドレス　クラス

インタフェース

：論理インタフェース名が表示されます。

要求ステート

：interfaceファイルに設定されている要求ステートが表示されます。

現在ステート

：現在の動作状態が表示されます。

最大送信長

：最大送信長が表示されます。

アドレス

：このインタフェースに割り当てられた自局IPアドレスが表示されます。

クラス

：このインタフェースがローカルインタフェースかどうかが表示されます。

(3) TCPのコネクション状態を表示する

TCPのコネクション状態の表示例

```
(1)ns> netstat ↓
 TCP CONNECTION STATUS
  LISTEN      <x  0, r  0> (0.0.0.0).23     <--> (0.0.0.0).0
  ESTABLISHED <x 10, r 24> (128.30.1.99).23 <--> (128.30.1.1).2049
  ESTABLISHED <x 10, r 24> (128.30.1.99).23 <--> (128.30.1.2).2050
(1)ns>
```

ステート　送信待バイト数　受信待バイト数　自局アドレス　自局ポート番号　相手アドレス　相手ポート番号

ステート

：TCPのコネクションの状態が表示されます。

ESTABLISHED	：コネクションが確立している状態
LISTEN	：相手からのコネクション待ち状態
SYN-SENT	：接続要求のSYNを送信した状態
SYN-RECEIVED	：接続要求を受信し、応答のSYNを送信した状態
FIN-WAIT-1	：切断要求のFINを送信した状態
FIN-WAIT-2	：本装置の切断は終了し、相手からの切断要求待ちの状態
CLOSE-WAIT	：相手からの切断要求を受け付け、本装置上のアプリケーションの切断要求待ち状態
TIME-WAIT	：切断後、そのポートを一定時間凍結している状態

送信待バイト数

：本装置のTCPが現在保持している送信データのバイト数が表示されます。

受信待バイト数

：本装置のTCPが現在保持している受信データのバイト数が表示されます。

自局アドレス

：自局のIPアドレスが表示されます。

自局ポート番号

：自局のポート番号が表示されます。

相手アドレス

：相手のIPアドレスが表示されます。

相手ポート番号

：相手のポート番号が表示されます。

(4) TCPの統計情報を表示する

TCPの統計情報の表示例

```
(1)ns> netstat -tcp↓
 TCP STATISTICS
        active open          0   ――――――   接続要求回数
        passive open         0   ――――――   接続受付回数
        input seg           29   ――――――   受信セグメント数
        input error          0   ――――――   エラーセグメント数
        retransmit           0   ――――――   再送回数
        output seg         592   ――――――   送信セグメント数
        output reset         1   ――――――   送信リセット数
(1)ns>
```

接続要求回数

：接続要求を行った回数が表示されます。

接続受付回数

：相手からの接続要求を受け付けた回数が表示されます。

受信セグメント数

：受信したTCPセグメント数が表示されます。

エラーセグメント数

：チェックサムエラーなどのエラーのあったTCPセグメント数が表示されます。

再送回数

：TCPが再送を行った回数が表示されます。

送信セグメント数

：送信したTCPセグメント数が表示されます。

送信リセット数

：送信したリセット数が表示されます。

(5) IPの統計情報を表示する

IPの統計情報の表示例

```
(1)ns> netstat -ip↓
  IP STATISTICS
         input datagram            561  —— 受信データグラム数
         output datagram           450  —— 送信データグラム数
         input error                 0  —— 受信エラー数
         forwarding datagram         0  —— フォワーディング数
  ICMP INPUT/OUTPUT STATISTICS      input      output
         destination unreachable       0          0
         time exceed                   0          0
         parameter problem             0          0
         source quench                 0          0
         redirect                      0          0
         echo message                  0          0
         echo reply                    0          0
         time stamp message            0          0
         time stamp reply              0          0
         address mask message          0          0
         address mask reply            0          0
(1)ns>
```

ICMP統計情報

受信データグラム数
：受信したIPデータグラム数が表示されます。

送信データグラム数
：送信したIPデータグラム数が表示されます。

受信エラー数
：チェックサムエラーなどのエラーとなったIPデータグラム数が表示されます。

フォワーディング数
：IPがフォワーディングしようとしたIPデータグラム数が表示されます。

ICMP統計情報

：ICMPの統計情報が表示されます。各ICMPパケットの送信および受信パケット数が表示されます。
以下にICMPメッセージの種類を示します。

destination unreachable	：	宛先未着メッセージ
time exceed	：	滞留時間超過メッセージ
parameter problem	：	パラメータエラーメッセージ
source quench	：	送信元抑制メッセージ
redirect	：	経路変更メッセージ
echo message	：	エコー要求メッセージ
echo reply	：	エコー応答メッセージ
time stamp message	：	タイムスタンプ要求メッセージ
time stamp reply	：	タイムスタンプ応答メッセージ
address mask message	：	アドレスマスク要求メッセージ
address mask reply	：	アドレスマスク応答メッセージ

(6) UDPの統計情報を表示する

UDPの統計情報の表示例

```
(1)ns> netstat -udp↓
 UDP STATISTICS
      input seg              0    ――  受信セグメント数
      input error            0    ――  受信エラー数
      output seg             0    ――  送信セグメント数
      port unreach          25    ――  ポート未着セグメント数
(1)ns>
```

受信セグメント数

：受信したUDPセグメント数が表示されます。

受信エラー数

：エラーのあったUDPセグメント数が表示されます。

送信セグメント数

：送信したUDPセグメント数が表示されます。

ポート未着セグメント数

：宛先ポートに到達できずに廃棄されたUDPセグメント数が表示されます。

(7) UDPの状態を表示する

UDPの状態の表示例

```
(1)ns> netstat -udpp↓
 UDP PORT STATUS
 (128.30.2.41).161 <--> (0.0.0.0).0
(1)ns>
```

自局アドレス　自局ポート番号　相手アドレス　相手ポート番号

自局アドレス
：自局のIPアドレスが表示されます。

自局ポート番号
：自局のポート番号が表示されます。

相手アドレス
：相手のIPアドレスが表示されます。

相手ポート番号
：相手のポート番号が表示されます。

(8) アクセスリストおよびアウトプットフィルタの統計情報を表示する

アクセスリストおよびアウトプットフィルタの統計情報の表示例

```
(1)ns> netstat -fil↓
INPUT/OUTPUT FILTER STATISTICS
 name     discarded by   discarded by
            access list      outputfil
 lo0            -----          -----
 sink0          -----          -----
 ipnhr0         -----          -----
 sink1          -----          -----
 en0                0          -----
 en1                0          -----
 ncp10            435             28
 ncp11              0            199
```

インタフェース　**アクセスリスト廃棄IPデータグラム数**　**アウトプットフィルタ廃棄IPデータグラム数**

インタフェース
：論理インタフェース名が表示されます。

アクセスリスト廃棄IPデータグラム数
：アクセスリストにより廃棄されたIPデータグラム数が表示されます。

アウトプットフィルタ廃棄IPデータグラム数
：アウトプットフィルタにより廃棄されたIPデータグラム数が表示されます。

注 意　**表示中の-----は各フィルタが設定されていないことを示します。**

注 意　**論理インタフェースncpxxは、pppが確立している場合のみ表示されます。また、統計情報には、その論理インタフェースncpxxが以前に使用された(pppが確立した)時の統計情報も含まれています(pppが切断されても統計情報はクリアされません)。**

page

機　　能　コマンドの画面表示を画面単位に区切ります。

フォーマット　page［-l　行数］コマンド

パラメータ
行数　：　1画面分の行数として扱う行数省略時は23行です。
コマンド　：　大量の画面表示を行う、本装置の統計表示などのコマンドです。具体的には、linestat、netstatなどです。

使 用 例　linestatの画面表示を10行単位に区切ります。

```
(1)ns> page -l 10 netstat -ip↓
 IP STATISTICS
        input datagram             151
        output datagram            107
        input error                  0
        forwarding datagram          3

 ICMP INPUT/OUTPUT STATISTICS        input     output
        destination unreachable          0          0
        time exceed                      0          0
        parameter problem                0          0
—More—
```

「--More--」の表示は画面表示を区切ったことを示しています。この表示のときにキー入力で以下の操作ができます。

スペース　：次の1画面面を表示します。
　　　　　　(上記の例では、次の10行を表示します)
リターン　：次の1行を表示します。
qまたはQ　：表示を終了します。

注　　意
・pageコマンドを途中で終了させると画面に「Broken pipe」が表示されることがありますが異常ではありません。
・「コマンド」にはeditコマンドなどのキー入力を行うコマンドを指定しないでください。そのようなコマンドは、pageコマンドと共には正しく動作できません。

passwd

機　　能　本装置にログインするためのパスワードを設定します。

フォーマット　passwd

パラメータ　なし

使 用 例　パスワードを設定する

```
(1)ns> passwd ↓
Enter New Password ? ____________↓
Re-Enter New Password ? ______________↓
(1)ns>
```

新しいパスワードを入力します。　**確認のために新しいパスワードを再度入力します。**

なお、パスワードはエコーされません。

注　　意　本装置にログインできなくなってしまいますので、設定したパスワードを忘れないように注意してください。

エ ラ ー

エラーメッセージ	意　味	対　処
Mismatch, password is not changed.	2回入力した新しいパスワードが一致しない。パスワードは変更されなかった。	再度passwdコマンドを実行してください。

解　　説　passwdコマンドは、本装置にログインするためのパスワードを設定するコマンドです。パスワードの設定は、各ユーザで本装置にログインしてから、passwdコマンドで設定してください。また、スーパーユーザのパスワードは、suコマンドでスーパーユーザになってからpasswdコマンドで設定してください。
設定したパスワードは次にログインするときから有効になります。

注　意　**passwdコマンドで変更した内容をセットアップカードにセーブするにはwriteコマンドを実行してください。writeコマンドを実行しないで、リブートしたりすると変更内容が失われてしまいます。**

注　意　**一般ユーザはpasswdコマンドで自分のパスワードを変更することができますが、writeコマンドでセットアップカードにセーブすることはできません。変更内容をセーブしたいときには、スーパーユーザに依頼してください。**

ping

機　　能　IPネットワーク上の相手ホストとの通信の確認を行います。

フォーマット　ping［-s　ソース IPアドレス］［-c　送信回数］［-l　データグラム・サイズ］［-i　送信間隔］［-t　TTL値］　相手ホスト名

パラメータ

-s　ソースIPアドレス	:	パケットのソースIPアドレス。省略時は、自局ホスト名に対応したIPアドレスになります。自局IPアドレスのいずれかである必要があります。
-c　送信回数	:	ICMP Echo Requestパケットの送信数。0を指定すると、永久に送信し続けます。「Ctrl 」+「C」で終了できます。省略時は、3個送信されます。
-l　データグラムサイズ	:	ICMPヘッダの後ろに付加されるデータ・バイト数。省略時は、40バイトになります。8バイト未満を指定すると、結果表示の時にround-tripの統計は含まれません。
-i　送信間隔	:	ICMP EchoRequestパケットの送信間隔。100 ms以上からms単位で指定します。省略時は、1sです。
-t　TTL値	:	IPヘッダの中のTime To Liveの値。0は無効で、256以上を指定すると自動的に60になります。省略時は、60です。
相手ホスト名	:	通信の確認を行う相手ホスト名またはIPアドレス。

使 用 例　(1) ホスト名「 host1」（IPアドレスが128.1.1.1）との通信を確認する場合

```
(1)ns>  ping  host1 ↓
Sending 3, 40-data byte ICMP Echos to 128.1.1.1

48 bytes from 128.1.1.1: seq=0 time=1 ms
48 bytes from 128.1.1.1: seq=1 time=1 ms
48 bytes from 128.1.1.1: seq=2 time=1 ms

—— 128.1.1.1 PING Statistics ——
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)   min/avg/max = 1/1/1
(1)ns>
```

48バイトのICMP Echo Replyパケットを3個受信したことを示します。

seqは受信したパケットのシーケンス番号、timeはEcho Requestパケットを送信してから、Echo Replyパケットを受信するまでの時間をms単位を表示しています。

指定された送信数が終わると、統計が表示されます。

3個のパケットを送信し、3個のパケットを受信し、受信できなかった応答パケット数を%表示しています。round-tripは、受信時に表示されるtime値の最小／平均／最大です。

(2) IPアドレスが130.1.1.1との通信を確認する場合

```
(1)ns>  ping  -c 5  -l 100  -i 500  130.1.1.1 ↓
Sending 5, 100-data byte ICMP Echos to 130.1.1.1

108 bytes from 130.1.1.1: seq=0 time=11 ms
108 bytes from 130.1.1.1: seq=1 time=11 ms
108 bytes from 130.1.1.1: seq=2 time=11 ms
108 bytes from 130.1.1.1: seq=3 time=11 ms
108 bytes from 130.1.1.1: seq=4 time=11 ms

―― 130.1.1.1 PING Statistics ――
5 packets transmitted,  5 packets received,  0% packet loss
round-trip (ms)   min/avg/max = 11/11/11
(1)ns>
```

(3) IPアドレスが130.1.1.1との通信が確認できない場合

```
(1)ns>  ping  130.1.1.1 ↓
Sending 3,  40-data byte ICMP Echos to 130.1.1.1

―― 130.1.1.1 PING Statistics ――
3 packets transmitted, 0 packets received, 100% packet loss
(1)ns>
```

3個のパケットを送信後10秒間受信を待ち、終了します。

解　　説　pingコマンドは、通信障害が発生した場合などに、それぞれのホストとの通信を確認して障害箇所の切り分けを行うときに有効なコマンドです。
pingコマンドは、IPネットワークに接続された相手ホストにICMPパケットを送信して、その応答を受信するコマンドです。相手ホストからの応答を受信できない原因としては、相手ホストが立ち上がっていない、本装置から相手ホストまでのネットワークの障害、ケーブルの接続不良などが考えられます。

pstat

機　　能　本装置のCPUの使用状況を表示します。

フォーマット　pstat

パラメータ　なし

使 用 例　CPUの使用状況を表示する

```
(1)ns> pstat↓
 28%  utilized (For five seconds)   ——  5秒間のCPUの使用率
 25%  utilized (For one minute)     ——  1分間のCPUの使用率
(1)ns>
```

解　　説　pstatコマンドは本装置のCPUの使用率を表示するコマンドです。
コマンドが入力された時点のシステム内の過去5秒間および1分間のCPUの使用率をパーセントで表示します。

5秒間のCPUの使用率
：過去5秒間のCPUの使用率を表示します。

1分間のCPUの使用率
：過去1分間のCPUの使用率を表示します。

radiusstat

機　　能　RADIUS認証サーバおよびRADIUSアカウントサーバに対する現在の状態を表示します。

フォーマット　radiusstat

パラメータ　なし

使 用 例　RADIUS認証サーバおよびRADIUSアカウントサーバに対する現在の状態を表示する

```
(1)ns> radiusstat↓
Mon Jan 10 14:22:26 JST 2000
<Radius Auth status>
MODE   HOST         CURRENT_HOST  CHANGED_TIME    RTIME
on     172.31.1.23  172.31.1.23   01/10 13:55:49      0
       172.31.1.102

<Radius Acct status>
MODE    HOST         CURRENT_HOST  CHANGED_TIME   RTIME
on      172.31.1.23  172.31.1.23   01/10 13:50:50     0
        172.31.1.102
```

解　　説　radiusstat は、RADIUS認証サーバおよびRADIUSアカウントサーバに対する現在の状態を表示するコマンドです。

(1) RADIUS認証サーバに対する現在の状態の表示

RADIUS認証サーバに対する現在の状態の表示例

```
<Radius Auth status>
MODE  HOST          CURRENT_HOST  CHANGED_TIME     RTIME
on    172.31.1.23   172.31.1.23   01/10 13:55:49       0
      172.31.1.102
```

モード　設定認証サーバ　認証サーバ　移行時刻　リセットタイム

モード

：RADIUS認証サーバを使用しているかどうかを表示します。
on ：　使用している
off ：　使用していない
radiusファイルのmodeキーワードの設定内容に対応しています。

設定認証サーバ

：設定されているRADIUS認証サーバのIPアドレスを表示します。
radiusファイルのhost1、host2、host3キーワードの順に表示しています。
設定されていない場合は、表示されません。

認証サーバ

：最後に応答があったRADIUS認証サーバのIPアドレスを表示します。
次回アクセスするRADIUS認証サーバであることを示します。
モードが「off」の場合は、「--.--.--.--」で表示されます。

移行時刻

：アクセスしていたRADIUS認証サーバが別のRADIUS認証サーバへ移行した時の時刻を表示します。
1度も移行がない場合は、「--/-- --:--:--」で表示されます。

リセットタイム

：プライマリRADIUS認証サーバ(*1)から別のRADIUS認証サーバに移行してから、プライマリRADIUS認証サーバに戻るまでの残り時間を秒単位で表示します。
移行した直後は、radiusファイルのrtimeキーワードの設定内容が設定されます。
rtimeが設定されていない場合は、「-」で表示されます。

(＊1)　プライマリRADIUS認証サーバ
HOSTの最上段に表示されるIPアドレスのRADIUS認証サーバです。

注 意　**CURRENT_HOSTで表示されているIPアドレスがプライマリRADIUS認証サーバではなく、RTIMEが「0」の場合は、次回アクセスするのは、プライマリRADIUS認証サーバになります。**

CHANGED_TIMEは、reloadコマンドでRADIUS認証サーバがプライマリRADIUS認証サーバに初期化された場合には更新されません。

(2) RADIUSアカウントサーバに対する現在の状態の表示

RADIUSアカウントサーバに対する現在の状態の表示例

```
<Radius Acct status>
MODE  HOST          CURRENT_HOST  CHANGED_TIME     RTIME
on    172.31.1.23   172.31.1.23   01/10 13:50:50       0
      172.31.1.102
```

設定アカウントサーバ　**移行時刻**
モード　**アカウントサーバ**　**リセットタイム**

モード

：RADIUSアカウントサーバを使用しているかどうかを表示します。
　on　：　使用している
　off　：　使用していない
radiusファイルのmodeキーワードの設定内容を表示しています。

設定アカウントサーバ

：設定されているRADIUSアカウントサーバのIPアドレスを表示します。
radiusファイルのhost1、host2、host3キーワードの順に表示しています。
設定されていない場合は、表示されません。

アカウントサーバ

：最後に応答があったRADIUSアカウントサーバのIPアドレスを表示します。
次回アクセスするRADIUSアカウントサーバであることを示します。
モードが「off」の場合は、「--.--.--.--」で表示されます。

移行時刻

：アクセスしていたRADIUSアカウントサーバが別のRADIUSアカウントサーバへ移行した時の時刻を表示します。
1度も移行がない場合は、「--/-- --:--:--」で表示されます。

リセットタイム

：プライマリRADIUSアカウントサーバ(*1)から別のRADIUSアカウントサーバに移行してから、プライマリRADIUSアカウントサーバに戻るまでの残り時間を秒単位で表示します。
移行した直後は、radiusファイルのrtimeキーワードの設定内容が設定されます。
rtimeが設定されていない場合は、「-」で表示されます。

(*1) プライマリRADIUSアカウントサーバ
HOSTの最上段に表示されるIPアドレスのRADIUSアカウントサーバです。

注 意　CURRENT_HOSTで表示されているIPアドレスがプライマリRADIUSアカウントサーバではなく、RTIMEが「0」の場合は、次回アクセスするのは、プライマリRADIUSアカウントサーバになります。

CHANGED_TIMEは、reloadコマンドでRADIUSアカウントサーバがプライマリRADIUSアカウントサーバに初期化された場合には更新されません。

reboot

機　　能　本装置をリブートします。

フォーマット　reboot

パラメータ　なし

使 用 例　本装置をリブートする

```
# reboot ↓
Do you really want to reboot [y/n] ?  y ↓
```

「y」を入力してからリブートが完了するまでにはしばらく時間がかかります。

注　　意　リブートを実行すると、edit、passwd、auth、clear、loadコマンドなどで変更したメモリー上の一時ファイルの内容は失われてしまいます。変更した内容を保存したい場合には、writeコマンドでセットアップカードに書き込んでからリブートしてください。

解　　説　rebootコマンドは、本装置をリブートするコマンドです。
本装置の変更したセットアップを有効にする場合などに、リブートを実行します。

CONSOLEポートに接続した端末からリブートする場合

```
# reboot ↓
Do you really want to reboot [y/n] ?  y ↓

login:
```

リブート終了後、リターンキーを押すとCONSOLEポートに接続した端末にプロンプトが表示されます。

「y」を入力するとリブートが実行されます。
「n」を入力するとリブートの実行は中止されます。

telnetでログインした端末からリブートする場合

```
# reboot ↓
Do you really want to reboot [y/n] ?  y ↓

connection closed by foreign host.
```

リブートを実行するとtelnetのコネクションが切断されます。ここで表示されるメッセージはログインしているホストによって異なります。

セットアップファイルを編集してwriteコマンドでセーブしていない場合

```
# reboot ↓
Setup files are modified. really reboot[y/n]? y ↓
```

reload

機　　能　本装置のいくつかのセットアップの変更内容を有効にします。

フォーマット　reload

パラメータ　なし

使 用 例　usersファイルの変更内容を有効にする。

usersファイルを変更する。
usersファイルの変更内容を有効にする。

```
# reload↓
#
```

解　　説　reloadコマンドは、セットアップファイルの変更内容を有効にするコマンドです。reloadコマンドで有効になるのは、interfaceファイル、gatewaysファイル、ipfiltersファイル、usersファイル、radiusファイル、ippoolファイル、rip.confファイルおよびboardsファイルの一部に対する変更です。

注　意　**reloadコマンドを実行すると、本装置内部の設定情報が再構築されます。このため、発信および着信が多い時にreloadコマンドを実行すると、発信および着信が失敗する場合があります。**

ripstat

機　　能　RIPの統計情報を表示します。

フォーマット
ripstat　global
ripstat　if　[論理インタフェース名]

パラメータ
global　　：グローバルな統計情報を表示します。
if　　：インタフェース毎の統計情報と設定を表示します。
論理インタフェース名　：統計情報を表示したい論理インタフェース名を指定します。省略すると、すべてのインタフェースについて統計情報と設定を表示します。

使 用 例　グローバルな統計情報を表示する

```
# ripstat global↓
Global Statistics
RouteChanges = 15, Queries = 0, BadPackets = 0
#
```

エ ラ ー

エラーメッセージ	意　　味	対　　処
ripstat: invalid interface [XXX]	論理インタフェース[XXX]の指定が不正です。	rip.confファイルの論理インタフェース名を確認してください。
ripstat: not found interface	指定された論理インタフェースが見つかりません。	rip.confファイルの論理インタフェース名を確認してください。

解　　説　ripstatコマンドは、RIPの統計情報を表示するコマンドです。
指定するパラメータによって、表示される内容は異なります。

(1) グローバルな統計情報の表示

送受信したRIPパケットのグローバルな統計情報を表示します。

グローバルな統計情報の表示例

```
# ripstat global↓
Global Statistics
RouteChanges = 15, Queries = 0, BadPackets = 0
#
```

RouteChanges
：ルートが変化した回数が表示されます。

Queries
：他のルータまたはホストから受信したRIPリクエストに対するRIPレスポンスの回数が表示されます。

BadPackets
：受信したRIPパケットの送信元が正しくない場合（ポート番号が違うまたはネットワークが違う場合）に廃棄したRIPパケットの数が表示されます。

(2) インタフェース毎の統計情報と設定情報の表示

送受信したRIPパケットの統計情報と設定情報を論理インタフェース毎に表示します。

インタフェース毎の統計情報と設定情報の表示例

```
# ripstat if↓
Interface Statistics & Configuration <en1>
 RcvBadRoutes = 0, Updates = 7
 bad_version = 0, bad_command = 0, bad_auth = 0
 rcv_packets = 52044, full_updates = 55495, transitions = 0
 AuthType = 0, AuthKey = , Send = 0x4, Receive = 0x6
Interface Statistics & Configuration <en0>
 RcvBadRoutes = 0, Updates = 7
 bad_version = 0, bad_command = 0, bad_auth = 0
 rcv_packets = 0, full_updates = 55495, transitions = 0
 AuthType = 0, AuthKey = , Send = 0x4, Receive = 0x6
#
# ripstat if en0↓
Interface Statistics & Configuration <en0> —— 論理インタフェース名
 RcvBadRoutes = 0, Updates = 7
 bad_version = 0, bad_command = 0, bad_auth = 0
 rcv_packets = 0, full_updates = 55511, transitions = 0
 AuthType = 0, AuthKey = , Send = 0x4, Receive = 0x6
#
```

論理インタフェース名

：論理インタフェース名が表示されます。

RcvBadRoutes

：受信したRIPパケット中のルートエントリで、アドレスファミリ不正、メトリック不正、宛先不正の理由で無視した数が表示されます。

Updates

：定期更新を含まないtriggered updateの回数が表示されます。

bad_version

：RIPを受信したインタフェースにおいて、受け入れない設定になっているバージョンまたは不正なバージョン(バージョン1、2以外)だった場合に廃棄したRIPパケットの数が表示されます。

bad_command

：受信したRIPパケットのコマンドが不正だった場合に廃棄したRIPパケットの数が表示されます。

bad_auth

：認証が失敗した場合に廃棄したRIPパケットの数が表示されます。

rcv_packets

：受信したRIPパケットの中で、廃棄せずに受け入れたRIPパケットの数が表示されます。

full_updates

：定期更新の回数が表示されます。

transitions

：インタフェースがアップ/ダウンした回数が表示されます。

AuthType

：認証タイプが表示されます。

0 ：認証なし

2 ：シンプルパスワード

AuthKey

：認証のパスワードが表示されます。
設定されていないときは何も表示されません。

Send

：そのインタフェースに設定されている送信の制御方法が表示されます。

0x1　：none
0x2　：rip1
0x4　：rip2
0x14 ：rip2mcast

Receive

：そのインタフェースに設定されている受信の制御方法が表示されます。

0x1　：none
0x2　：rip1
0x4　：rip2
0x6　：both

riptrace

機　　能　送受信したRIPパケットの内容をコンソールに出力します。

フォーマット　riptrace　on | detail | off

パラメータ

- on　：RIPパケットを送受信した場合に、バージョン、コマンド名、送信先/送信元のIPアドレス、ポート番号をコンソールに出力します。
- detail　：RIPパケットを送受信した場合に、バージョン、コマンド名、送信先/送信元のIPアドレス、ポート番号とルートエントリをコンソールに出力します。
- off　：RIPパケットを送受信した場合に、何もコンソールに出力しません。

使 用 例　送受信したRIPパケットをコンソールに出力する

```
# riptrace detail↓
# @T(5/15 15.39.24):routed: v2 RESPONSE from 172.31.3.101,520
        dst 0.0.0.0         mask 00000000 next 0.0.0.0    metric  4 tag 0
@T(5/15 15.39.29):routed: v2 RESPONSE to 172.30.255.255,520 (en1)
        dst 172.31.0.0      mask FFFF0000 next 0.0.0.0    metric  1 tag 0
        dst 0.0.0.0         mask 00000000 next 0.0.0.0    metric  4 tag 0
@T(5/15 15.39.29):routed: v2 RESPONSE to 172.31.255.255,520 (en0)
        dst 172.20.0.0      mask FFFF0000 next 0.0.0.0    metric  3 tag 0
        dst 172.30.0.0      mask FFFF0000 next 0.0.0.0    metric  1 tag 0
        dst 0.0.0.0         mask 00000000 next 0.0.0.0    metric  4 tag 0
@T(5/15 15.39.31):routed: v1 RESPONSE from 172.30.2.2,520
        dst 0.0.0.0         mask 00000000 next 0.0.0.0    metric 16 tag 0
        dst 172.31.0.0      mask 00000000 next 0.0.0.0    metric 16 tag 0
        dst 172.20.0.0      mask 00000000 next 0.0.0.0    metric  2 tag 0
```

解　　説　riptraceコマンドは、送受信したRIPパケットをコンソールに出力するコマンドです。

送受信したRIPパケットの表示例

```
# riptrace on ↓
# @T(5/16 11.26.52):routed: v1 RESPONSE from 172.30.2.2,520
@T(5/16 11.26.53):routed: v2 RESPONSE from 172.31.3.101,520
@T(5/16 11.26.58):routed: v2 RESPONSE to 172.30.255.255,520 (en1)
@T(5/16 11.26.58):routed: v2 RESPONSE to 172.31.255.255,520 (en0)
```

バージョン　コマンド名　送信先/送信元　ポート番号

送受信したRIPパケットの詳細な表示例

```
# riptrace detail↓
# @T(5/16 13.26.1):routed: v2 RESPONSE to 172.31.255.255,520 (en0)
        dst 172.20.0.0     mask FFFF0000 next 0.0.0.0     metric  3 tag 0
        dst 172.30.0.0     mask FFFF0000 next 0.0.0.0     metric  1 tag 0
        dst 0.0.0.0        mask 00000000 next 0.0.0.0     metric  4 tag 0
@T(5/16 13.26.10):routed: v1 RESPONSE from 172.30.2.2,520
        dst 0.0.0.0        mask 00000000 next 0.0.0.0     metric 16 tag 0
        dst 172.31.0.0     mask 00000000 next 0.0.0.0     metric 16 tag 0
        dst 172.20.0.0     mask 00000000 next 0.0.0.0     metric  2 tag 0
@T(5/16 13.26.26):routed: v2 RESPONSE from 172.31.3.101,520
        dst 0.0.0.0        mask 00000000 next 0.0.0.0     metric  4 tag 0
@T(5/16 13.26.31):routed: v2 RESPONSE to 172.30.255.255,520 (en1)
        authtype 2
        dst 172.31.0.0     mask FFFF0000 next 0.0.0.0     metric  1 tag 0
        dst 0.0.0.0        mask 00000000 next 0.0.0.0     metric  4 tag 0
```

宛先アドレス　認証タイプ　マスク　ネクストホップ　メトリック　ルートタグ

バージョン

：送受信したRIPパケットのバージョン番号が表示されます。

コマンド名

：送受信したRIPパケットのコマンド名が表示されます。

送信先/送信元

：受信したRIPパケットの場合には「from　<送信元のIPアドレス>」、送信したRIPパケットの場合には「to　<送信先のIPアドレス>」が表示されます。

ポート番号

：RIPパケットの送信先または送信元のポート番号が表示されます。

認証タイプ

：認証タイプが表示されます。認証を行わない設定の場合は、表示されません。

2：シンプルパスワード

宛先アドレス

：宛先IPアドレスが表示されます。

マスク

：宛先IPアドレスに対するマスクが表示されます。

ネクストホップ

：宛先へのパケットをフォワーディングすべき次のホップが表示されます。
0.0.0.0の場合は、このRIPパケットの送信元が経由すべき次のホップであることを示します。

メトリック

：そのルートのメトリックが表示されます。

ルートタグ

：そのルートのルートタグが表示されます。

show

機　　能　セットアップファイルの内容を表示します。

フォーマット

show　[-a]　[-n]　ファイル名

show　[-h]

パラメータ

-a	：	ページごとに表示を中断しない
-n	：	行番号を付加する
-h	：	セットアップファイルの一覧を表示する
ファイル名	：	表示するファイル名

使 用 例

hostnameファイルの内容を表示する

```
# show  hostname↓
router_A
#
```

行番号付きでhostnameファイルの内容を表示する

```
# show  -n  hostname↓
0001  router_A
#
```

セットアップファイルの一覧を表示する

```
# show  -h↓
# IP
   gateways IP Static Gateway Information
              ・
              ・
              ・
#
```

解　　説　showコマンドは、ファイルの内容を表示するコマンドです。
表示するファイルが画面の1ページ (=23行) 以内の場合には、ファイルの内容を表示してコマンドが終了します。
表示するファイルが画面の1ページ (=23行) 以上の大きさの場合には、1ページずつ表示し、キー入力待ちになります。ここで、次のページを表示する場合には、スペースを入力します。コマンドを終了する場合には、「q」を入力します。

(1) 1ページずつの表示

1ページ (=23行) 以上のファイルを指定した場合には、1ページずつ表示されます。そこでスペースを入力すると次のページが表示されます。

1ページ以上のファイルの表示例

```
# show  hosts↓
#
#  internet hosts
#
128.30.0.99   router_A
          •
          •
          •
   enter  space:next page   'q':quit  ? _
```

ここで、スペースを入力すると次のページが表示される。
「q」を入力するとコマンドが終了する。

次のページの表示例（スペースを入力した場合）

```
128.31.1.1   ws1
128.31.1.2   ws2
#
128.31.2.1   pc1
          •
          •
          •
   enter  space:next page   'q':quit  ?
```

表示後も次のページがある場合には、再度、プロンプトが表示される。

(2) セットアップファイルの一覧表示

セットアップファイルの一覧を表示する

```
# show -h↓
# IP
   gateways      IP Static Gateway Information
   interface     IP Direct Attached segment Information
   hostname      My Host Name
   hosts         Host Name and its IP-address
   netmask       IP Subnet Mask
   ipfilters     IP Packet Filter
   resolv.conf   Domain Name System
   services      Service Name and Port Number
   snmpconf      SNMP Parameters
   rip.conf      RIP Configuration
   syslog.conf   SYSLOG Configuration
# WAN
   boards        Extention Board Configurations
   users         Remote User Configurations
   radius        RADIUS Server Parameters
   ippool        IP Pool Configurations
# ETC.
   servers       Server Programs
```

shutdown

機　　能　本装置をシャットダウンします。

フォーマット　shutdown

パラメータ　なし

使 用 例　本装置をシャットダウンする

```
# shutdown↓
Do you really want to shutdown [y/n] ?  y↓
```

「y」を入力してからシャットダウンが完了するまではしばらく時間がかかります。

注　　意　shutdownコマンドを実行しないで、本装置の電源をOFFにしたり、システムメモリカードを抜いた場合には、メモリカードの内容が破壊される場合があります。

解　　説　shutdownコマンドは、本装置をシャットダウンするコマンドです。
シャットダウンすると本装置の機能はすべて停止し、本装置を介して通信している装置は、通信ができなくなります。本装置を停止しても構わないことを確認してからシャットダウンしてください。

本装置の電源をOFFにする場合や、システムメモリカードを抜く場合には、必ずshutdownコマンドを実行して、シャットダウンが終了したことを確認してから行ってください。
シャットダウンの終了は、ステータスランプ4が点滅することで確認してください。

CONSOLEポートに接続した端末からシャットダウンする場合

```
# shutdown↓
 Do you really want to shutdown [y/n] ?  y↓


 MON>
```

「y」を入力するとシャットダウンが実行されます。
「n」を入力するとシャットダウンの実行は中止されます。

シャットダウン終了後、リターンキーを押すとCONSOLEポートに接続した端末にプロンプト「MON>」が表示されます。

telnetでログインした端末からシャットダウンする場合

```
# shutdown↓
Do you really want to shutdown [y/n] ?  y↓


connection closed by foreign host.
```

シャットダウンを実行するとtelnetのコネクションが切断されます。ここで表示されるメッセージはログインしているホストによって異なります。

snmpreload

機　　能　snmpcomfファイルの変更内容を有効にします。
（snmprestartコマンドとは異なり、snmpdの再起動は行いません。）

フォーマット　snmpreload

パラメータ　なし

使 用 例

```
# snmpreload↓
#
```

解　　説　snmpreloadコマンドは、snmpconfファイルの変更内容を有効にするコマンドです。ただし、trapとcommunityキーワード以外のキーワードを削除した場合は、前回の設定内容が有効になります。

serversファイルの設定変更でsnmpdを使用するか否かを切り換える場合は、snmprestartコマンドを使用します。

snmprestart

機　　能　SNMPを再起動します。

フォーマット　snmprestart

パラメータ　なし

使 用 例

```
# snmprestart↓
#
```

解　　説　snmprestartコマンドは、SNMPを再起動するコマンドです。
再起動する際、serversファイルにSNMPを起動する設定になっている場合は、SNMPを起動し、snmpconfファイルの内容が再読み込みされます。

statclear

機　　能　下記統計表示コマンドが表示する値をリセットします。

linestat　-s
linestat isdn　-s | -s2
netstat　-ip
netstat　-tcp
netstat　-udp

フォーマット　statclear

パラメータ　なし

使 用 例

```
# statclear↓
#
```

注　　意　statclearの実行後は、各統計表示コマンドは、statclearが最後に実行されたときからの相対時間も表示されます。

netstatコマンドを例に、画面表示例を下記に示します。

例1　statclearの実行前の「netstat -ip」の表示

```
(1)ns> netstat -ip↓
  IP STATISTICS
         input datagram          561
         output datagram         450
         input error               0
         forwarding datagram       0
ICMP INPUT/OUTPUT STATISTICS   input   output
         destination unreachable   0        0
         time exceed               0        0
         parameter problem         0        0
         source quench             0        0
```

```
        redirect                    0        0
        echo message                0        0
        echo reply                  0        0
        time stamp message          0        0
        time stamp reply            0        0
        address mask message        0        0
        address mask reply          0        0
(1)ns>
```

例2　statclearの実行後の「netstat -ip」の表示
　　　（この場合の経過時間は、0日0時間3分4秒）

```
<< Time(0.00:03:04) >>
(1)ns> netstat -ip↓
  IP STATISTICS
        input datagram            561
        output datagram           450
        input error                 0
        forwarding datagram         0
ICMP INPUT/OUTPUT STATISTICS   input   output
        destination unreachable   0        0
        time exceed                 0        0
        parameter problem           0        0
        source quench               0        0
        redirect                    0        0
        echo message                0        0
        echo reply                  0        0
        time stamp message          0        0
        time stamp reply            0        0
        address mask message        0        0
        address mask reply          0        0
(1)ns>
```

解　　説　この機能は、正確にはカウンタのリセットではなく、現時点の統計値を内部に保存し、以降の表示で差分を表示させる機能です。

統計表示コマンド類を使う上では、カウンタがリセットされている様に見えますが、実際にはシステム内部のカウンタはリセットされていません。一方、snmpが示す値は、この操作には影響されず、装置が起動してからの積算値です。

su

機　　能　スーパーユーザにログインします。

フォーマット　su

パラメータ　なし

使　用　例　スーパーユーザにログインする

```
(1)ns> su↓
passwd:____________↓
#
```

解　　説　suコマンドは、スーパーユーザにログインするコマンドです。スーパーユーザになると、プロンプトが「#」になります。
スーパーユーザは、本装置の設定を変更したり、ユーザを登録したり、設定をセットアップカードに保存したりすることができるユーザです。スーパーユーザは一般ユーザが使用できないコマンドを使用することができます。
システムの保全のためには、スーパーユーザにはパスワードを必ず設定するほうが良いでしょう。

telnet

機　　能　telnetクライアントで相手ホストにログインします。

フォーマット　telnet［-s　ソースIPアドレス］相手ホスト名

パラメータ

ソースIPアドレス　：　パケットのソースIPアドレス。省略時は自局ホスト名に対応したIPアドレスになります。自局IPアドレスのいずれかである必要があります。

相手ホスト名　：　ログインする相手のホスト名またはIPアドレス

使 用 例　telnetでホスト名「host1」にログインする

```
(1)ns> telnet  host1↓
connect to [128.30.1.1:telnet]
connect complete

host1 login: user1    ---  host1が表示するログインプロンプト
password:
```

エ ラ ー　(1 / 2)

エラーメッセージ	意　味	対　処
Connection timed out	コネクションの開設でタイムアウトが発生した	指定したホストが立ち上がっているかネットワークケーブルが正しく接続されているかを確認してください。
Connection refused	コネクションの開設が拒否された	相手のホストでtelnetサーバが立ち上がっているか確認してください。
Network is unreachable	指定したホストのネットワークまで到達できない	① 指定したホスト名が正しいか確認してください。 ② gatewaysファイルの設定が正しいか確認してください。
Unknown host	指定したホスト名が見つからない	① 指定したホスト名が正しいか、hostsファイルに登録されているかを確認してください。 ② ドメインネームシステムを使用している場合にはドメインサーバ上のホスト名の登録を確認してください。

(2 / 2)

エラーメッセージ	意　　味	対　　処
No route to host	指定したホストへのルートがない	① 指定したホスト名が正しいか確認してください。 ② gatewaysファイルの設定が正しいか確認してください。 ③ ISDN経由のホストの接続の場合、usersファイルの設定が正しいか確認してください。

解　　説　telnetコマンドは、telnetプロトコルでIPネットワーク上のホストにログインするコマンドです。
telnetコマンドを用いて本装置と相手ホストの接続を確認したり、相手ホストにログインして状態を確認したりできます。
また、本装置はtelnetサーバをサポートしていますので、本装置のIPネットワークの設定をしている場合には、telnetコマンドを用いて本装置どうしでログインすることができます。

traceroute

機　　能　指定したホストに到達するためのルートを検査し、ルートが経由するルータのIPアドレス（またはホスト名）と、そのルータまでのパケットの往復時間（ミリ秒単位）の実測値を表示します。

フォーマット　traceroute [-n] [-p ポート番号] [-s ソースIPアドレス] [-m 最大ホップ数] [-q 検査回数] [-w 待ち時間]ホスト

パラメータ

-n ：検査結果の表示で、IPアドレスの代わりにホスト名を表示します。省略時はIPアドレスで表示します。

[注意]

このオプションを指定してホスト名を表示できるのは、hostsファイルに該当するホスト名が登録がされている場合と、ドメインネームシステムでホスト名が取得できた場合だけです。

-p　ポート番号 ：検査のパケットが使用する一連のデスティネーションポート番号の始まりの番号です。
省略時は30000です。

[注意]

検査のパケットが使用する一連のポート番号の範囲は「-p ポート番号」の値から「-p ポート番号」＋（「-q 検査回数」×「-m 最大ホップ数」－1）までです。
これらのポート番号はデスティネーションのホストで使用されていてはなりません。

-s　ソースIPアドレス：パケットのソースIPアドレスです。省略時は自局ホスト名に対応するIPアドレスになります。

[注意]

このアドレスは、自局が持つIPアドレスのうちのどれかでなければなりません。

-m　最大ホップ数 ：最大ホップ先のルータまで検査するかを指定します。
省略時は最大30ホップです。

-q　検査回数 ：検査回数です。省略時は3回です。

-w　待ち時間 ：応答パケットの待ち時間（秒単位）です。
省略時は5秒です。

ホスト　　　　　　　　：検査したいルートのデスティネーションとなるホストです。ホスト名またはIPアドレスで指定します。

使 用 例　130.31.1.30までのルートを調べます。

```
(1)ns> traceroute 130.31.1.30↓
  1:172.31.1.41   3   172.31.1.41   4    172.31.1.41   3
  2:10.5.24.1     3   10.5.24.1     3    10.5.24.1     3
  3:130.61.101.1  5   130.61.101.1  3    130.61.101.1  3
  4:130.10.31.1   3   130.10.31.1   3    130.10.31.1   3
  5:130.31.1.30   4        *             130.31.1.30   4
(1)ns>
```

130.31.1.30までのルートが「172.31.1.41」→「10.5.24.1」→「130.61.101.1」→「130.10.31.1」→「130.31.1.30」であることを示しています。

5ホップ目(130.31.1.30)までの往復時間の表示が
「5:130.31.1.30　　4　　*　　130.31.1.30　　　4」
となっています。これは1回目と3回目の検査結果が、それぞれ4ミリ秒で、2回目の検査では、応答が待ち時間内に得られなかったことを示しています。

エ ラ ー　デスティネーションまでのルートが分からないとき（無いとき）、「no route」が表示されます。

自局で全くルートが分からないときの表示例

```
(1)ns> traceroute 130.31.1.30↓
no route
(1)ns>
```

10.5.24.1から先のルートが分からないときの表示例

```
(1)ns> traceroute 130.31.1.30↓
  1:172.31.1.41    3   4   3
  2:10.5.24.1      3   3   3
no route
(1)ns>
```

version

機　　能　システムソフトウェアのバージョンを表示します。

フォーマット　version

パラメータ　なし

使 用 例　システムソフトウェアのバージョンを表示する

```
# version↓
# Multiservice Platform NS-4200-10 System Software 2001.xx.xx (Ver X.X)
```

wanport

機　　能　指定したPRIポートを、一時的にenable状態／disable状態にします。

フォーマット　wanport enable | disable 拡張ボードスロット番号-ポート番号 | all

パラメータ

enable	：	指定したPRIポートをenable状態にする
disable	：	指定したPRIポートをdisable状態にする
拡張ボードスロット番号	：	enable／disableするPRIポートが収容されている拡張ボードの拡張ボードスロット番号を指定する
ポート番号	：	enable／disableするPRIポートの番号を指定する
all	：	すべてのPRIポートをenable／disableする

使 用 例

すべてのPRIポートをdisable状態にする。

```
# wanport disable all↓
#
```

拡張ボードスロット1のPRIポート1をenable状態にする。

```
# wanport enable 1-1↓
#
```

解　　説

wanportコマンドは、一時的にPRIポートをenable状態あるいはdisable状態にするためのコマンドです。
本装置では、PRIポートをenable（ISDNの発信／着信が可能な状態）にするか、disable（ISDNの発信／着信ができない状態）にするかは、boardsファイルに設定します。
このwanportコマンドを使用すると、boardsファイルでenableに設定されているPRIポートをdisable状態にしたり、逆にboardsファイルでdisableに設定されているPRIポートをenable状態にすることができます。
たとえば、本装置のメンテナンスのために、新たな着信を受け付けたくない場合には、

```
# wanport disable all↓
```

と実行することによって、以後のISDNの新たな着信はすべて拒否されます。ただし、コマンドを実行する時点で接続されていた呼は、その呼が切断されるまで維持されます。

注　意　　wanportコマンドで一時的にPRIポートのenable／disableの状態を変更した場合、その後reloadコマンドを実行すると、boardsファイルに設定されているenable／disableの状態に戻ります。

関　連　　boardsファイル

参　照　　「5章　5.3」

write

機　　能　設定したファイルをセットアップカードに保存します。

フォーマット　write [領域]

パラメータ

省略時　：ブート時の領域に保存する

領域　：指定した領域に保存する（1または2）

使 用 例　設定したファイルをセットアップカードに書き込む

```
# write↓
#
```

解　　説　writeコマンドは、エディタなどで設定したファイルをセットアップカードに書き込むコマンドです。writeコマンドでセットアップカードに書き込んでおけば、本装置の電源をオフにしても設定内容は保存されます。次に立ち上げたときにも同様の設定で立ち上がります。

注　意　**writeコマンドの実行中に本装置の電源をオフにしたり、RESETスイッチを押したり、リブートしたりしないでください。セットアップカードが壊れてしまいます。**

以下のコマンドは、一時ファイルのみを変更します。したがって変更内容をセットアップカードに保存するためには、writeコマンドを実行する必要があります。

auth
clear
edit
load
passwd

セットアップカードには、ファイルを保存するための領域が2つあります。この2つの領域に異なる2種類のセットアップを保存することができます。通常は領域1のみが使用されます。現在の設定内容はそのまま保存しておき、試験的／一時的に異なる設定をしたい場合には領域2を使用すると便利です。領域2に試験的／一時的な設定を保存して動作を確認し、OKとなった時点で領域1に保存できます。

(1) ブート時の領域に保存する場合

設定したファイルをセットアップカードに保存する

```
# write↓
#
```

writeコマンドにパラメータを指定しない場合には、ブート時に使用された領域に保存されます。通常の立ち上げ方の場合には領域1が使用されます。領域2を使用する場合には、次の**(2)**を参照してください。

(2) 指定した領域に保存する場合

設定したファイルをセットアップカードの領域2に保存する

```
# write  2↓
#
```

領域2に保存した設定ファイルで立ち上げるには、以下のようにしてください。

・shutdownコマンドで本装置のシステムソフトウェアをストップする。
・CONSOLEポートに接続した端末から「↓」リターンを入力する。
・プロンプト「MON>」が表示される。
・「b -R2↓」を入力する。
・ブートが開始され、領域2の設定で立ち上がります。

```
MON > b  -R2↓
```

7章
トラブルシューティング

7章では、本装置に何らかのトラブルが発生したときの対処方法を説明しています。

本章の内容

7.1 トラブル処理の概要

本装置のトラブルは、本装置のハードウェアの異常と通信に関するトラブルに切り分けられます。本装置に何らかのトラブルが発生した場合は、その症状あるいは現象から判断して対応してください。

	参照項
電源が入らない	→ **7.2.1**
立ち上がらない / ブートできない	→ **7.2.2**
ステータスランプが点灯または点滅している	→ **7.2.3**
冷却ファンの音が以前より大きくなった / 冷却ファンが止まっている	→ **7.2.4**
通信ができない	→ **7.3**
エラーメッセージが表示されている	→ **7.3.1、付録B**
通信エラーの原因が特定できない	→ **7.3.4**

また、弊社ホームページ内の以下のURLの「技術情報」には、本装置のFAQ、設定事例集などが掲載されていますので、そちらもご参照ください。

http://www.sii.co.jp/js/nshp/

7.2　本装置のハードウェアに関連するトラブル

7.2.1　電源が入らない

・ 電源ケーブルは接続されていますか？
・ 電源スイッチはONになっていますか？
・ コンセントに電源が供給されていますか？

以上の確認をしても電源が入らない場合には、本装置の故障と考えられますので修理が必要です。速やかに電源スイッチをOFFにして、電源ケーブルをはずしてください。

7.2.2　立ち上がらない / ブートできない

・ 電源は入っていますか？
・ セットアップカードが入っていますか？

以上の確認をしても立ち上がらない場合には、ステータスランプの状態を確認してください。

点灯または点滅している	→	**7.2.3**へ
両方とも消灯している	→	本装置は立ち上がっているか、ROMモニタ動作中と考えられます。

7.2.3 ステータスランプが点灯または点滅している

ステータスランプ								意　味	対 処
1	2	3	4	5	6	7	8		
●	●	●	●	●	●	●	●	電源スイッチON直後	A
●	○	○	○	○	○	○	○	自己診断テスト (POC) 実行中 (約10秒)	B
○	●	○	○	○	○	○	○	拡張ボードの自己診断テスト実行中	B
○	○	●	○	○	○	○	○	ブート実行中	C
○	○	○	●	○	○	○	○	ブート実行中2	C
○	○	○	○	○	○	○	○	ブート正常終了	―
◎	○	○	○	○	○	○	○	自己診断テストのエラー	D
○	◎	○	○	○	○	○	○	拡張ボードの自己診断テストのエラー	D
○	○	◎	○	○	○	○	○	ブート中のエラー	E
○	○	○	◎	○	○	○	○	ブート中のエラー、システムソフトウェアのエラー	E

○ 消灯　● 点灯　◎ 点滅

対 処	対　処　方　法
A	電源スイッチをONにした直後には、一瞬この状態になります。電源スイッチをONにしてから、この状態のままならば本装置の故障と考えられますので修理が必要です。
B	1分以上待ってもこの状態のままならば、本装置の故障と考えられますので修理が必要です。
C	10分以上待ってもこの状態のままならば、本装置の故障と考えられます。
D	本装置の故障と考えられますので修理が必要です。
E	CONSOLEポートに端末を接続して、「↓」を入力するとROMモニタのプロンプト「MON>」が表示されます。 「e↓」を入力してエラーの原因を確認してください。 「OS: Shutdown complete.」と表示されたときには、本装置のシャットダウンが終了したことを示しています。この場合は、特に対応する必要は、ありません。 また、CONSOLEポートに端末を接続したまま、電源を入れ直して立ち上げてください。端末にコンソール出力が表示されますので、エラーが表示されていないか確認してください。

7.2.4 冷却ファンの異常音

冷却ファンは消耗品ですから経年変化によって劣化します。
冷却ファンの音が以前より著しく大きくなった場合には、最寄りのサービス拠点に修理を依頼してください。
また、電源をONにしても冷却ファンが止まっている場合には、本装置の故障の原因となりますので、電源をOFFにして、最寄りのサービス拠点にファンの交換を依頼してください。冷却ファンを交換するまでは使用しないでください。

7.3　通信に関連するトラブル

ここでは、本装置の通信機能に関するトラブルが発生した場合の切り分けを行うためのチェックポイントについて説明します。
本装置の通信機能に関連するトラブルシューティングにおける切り分け手段として、以下の手段があります。

- コンソールに出力されているメッセージの確認
  この確認によって、本装置の起動時あるいは通信中にエラーが発生している場合に、そのエラー内容を確認することができます。
- 本装置のランプの状態によるケーブル接続／通信状態の確認
  この確認によって、ケーブルが正しく接続されているかどうか、あるいは物理的な障害が発生しているかどうかの簡単なチェックが行えます。
- メンテナンスコマンドによる通信状態の確認
  コマンドの表示内容によって、本装置の現在の通信状態あるいは統計情報を確認することができます。

まずこれらの切り分け手段について、**7.3.1～7.3.3**で説明した後に、**7.3.4**で具体的な切り分け手順について説明します。

7.3.1　コンソールメッセージの確認

本装置のコンソールには、設定の誤りや通信時に発生した障害、エラーなど、トラブルシューティングに役に立つメッセージが表示されます。トラブルシューティングにあたっては、このコンソールに表示されるメッセージを確認してください。

(1) コンソールメッセージの確認方法

本装置のコンソールメッセージは、起動時には本装置のCONSOLEポートに接続されている端末（ターミナルソフトをもつパソコンなど）に表示されます。
またtelnetを使用して、ネットワーク上のホストから本装置にログインして、suコマンドでスーパーユーザになった後にconsoleコマンド（「console」と入力する）を実行すると、そのホストにコンソールメッセージを表示することもできます。

いずれの場合においても、suコマンドでスーパーユーザになった後に、「console -rev 10000」と入力することによって、すでにコンソールに表示されていたコンソールメッセージを確認することができます。**(2)**項の表示例では、telnetで本装置にログインして過去のコンソールメッセージを確認しています。（consoleコマンドの使用方法は、**「6章　コマンド・リファレンス」**を参照してください。）

(2) 本装置の起動時のエラーメッセージの確認

本装置のセットアップファイルの設定に誤りがある場合には、起動時にそのエラーメッセージがコンソールに表示されます。

本装置起動後にその内容を確認する場合、本装置にログインしてスーパーユーザになった後に、以下の表示例のように「console -rev 10000」を入力します。

usersファイルの設定に誤りがある場合の表示例

```
1 aya:manager> telnet ns4200
Trying 172.31.2.240 ...
Connected to ns4200.
Escape character is '^]'.
login :somebody
passwd:
(P1) ns4200 >su
passwd:
#
# console -rev 10000

checking file system.
（省略）
setting up network.
setting up LAN1 port.
setting up LAN2 port.
.............................................................
Slot(1):  completion.
sessionid=0x68000000

setting up wan config..
users(line 22):invalid keyword(remote_user)                          ←エラーメッセージ
users(line 25):This %user isn’t specified remote_name & remote_tel  ←エラーメッセージ
starting net services.
telnetd: start listen[telnet]
snmp: SNMP agent start.
acctd:start.
radiusd:start.
login :

@W(1/16 22.10.37):telnetd:incoming connection from (172.31.1.4), allocate ttyp1

@W(1/16 22.10.44):login:successful (somebody/ttyp1)

@W(1/16 22.10.45):COMMAND(su) invoked by somebody/ttyp1

@W(1/16 22.10.45):su:successful (somebody/ttyp1)
```

エラーメッセージが表示されている場合には、まずセットアップファイルの設定を確認して修正してください。

(2) 通信中に発生したWarningメッセージの確認方法

何らかの理由により通信中に通信エラーが発生すると、Warningメッセージがコンソールに表示されます。この場合にも、本装置にログインしてスーパーユーザになった後に、以下の表示例のように「console -rev 10000」と入力すれば、その内容を確認することができます。

接続相手のPPP認証のパスワードが間違っていた場合の表示例

```
# console –rev 10000
@W(1/14 11.18.24):authd:CHAP refuse(Invalid Response<take>)    ←Warningメッセージ
```

Warningメッセージが表示されている場合には、**「付録B エラーメッセージ一覧」**を参照してください。

7.3.2　ケーブルの接続の確認

何らかの通信障害が発生し、特に全くISDNから接続できない場合あるいはLAN上のホストと全く通信できない場合には、LANポート／PRIポートのケーブルの接続状態を確認してください。
なお、本装置の外観、ランプの名称については**「1.3　各部の名称と機能」**、ケーブルの接続方法については**「マルチサービス・プラットホームXtrax (NS-4200)設置手順書」**を参照してください。

(1) LANポートのケーブルの確認

本装置のLAN1ポート／LAN2ポートのケーブルの接続に関して、以下の項目を確認してください。

表7-1　LANポートのケーブル接続に関連するチェック項目

チェック項目	対処方法
イーサネット上にフレームが流れている時に、本装置のTXランプやRXランプが点滅していることを確認してください。	消灯したままである場合には、イーサネットケーブルが正しく接続されているか確認してください。
LINKランプが点灯していることを確認してください。	消灯している場合には、イーサネットケーブルが正しく接続されているか確認してください。またHUBがリンクビートテストをサポートしていることを確認してください（本装置はリンクビートテストをサポートしていないHUBと接続できません）。
100MのHUBあるいはスイッチングHUBに接続している場合、100BASE-TXランプが点灯していることを確認してください。	消灯している場合、イーサネットケーブルが正しく接続されているか、また接続しているHUBあるいはスイッチングHUBが100BASE-TXをサポートしているか、確認してください。

(2) PRIポートのケーブルの確認

本装置のPRIポートのケーブルの接続に関して、以下の項目を確認してください。

表7-2　PRIポートのケーブル接続に関連するチェック項目

チェック項目	対処方法
使用しているPRI拡張ボードのPRIランプが点灯していることを確認してください。	消灯している場合には、PRIポートが使用可能な状態になっていません。PRIケーブルが正しく接続されているか確認してください。またDSUの電源が入っているか確認してください。
使用しているケーブルが、本装置添付のPRIケーブルであることを確認してください。	本装置添付のケーブルではない場合、配線の相違から通信できない場合があります。本装置添付のPRIケーブルを使用してください。

7.3.3　メンテナンス用コマンドによる通信状態の確認

本装置では、以下のコマンドを使用することによって、本装置の現在の通信状態あるいは統計情報を確認することができます。ここでは、トラブルシューティングを行う場合に、トラブルの状況を把握するために有効な以下のコマンドについて、表示例と表示内容について説明します。なお各コマンドの詳細な使用方法、表示内容の意味については、**「6章　コマンド・リファレンス」**の各コマンドの項を参照してください。

コマンド	表示内容
linestat -P	ISDN回線および高速ディジタル回線のlayer1の状態
linestat isdn	現在のISDNの接続状態
linestat isdn -s	ISDN接続の統計情報
modemstat	現在のモデムあるいはPIAFSの接続状態
linestat	現在のPPPの接続状態
netstat -r	現在のrouting情報

上記コマンドの表示例を以下に示します。
この表示例は、

- 本装置にNS-420 PRI拡張ボードを拡張ボードスロット1に実装されている
- 本装置にNS-421-10/30 DSP拡張ボードが2枚実装されている
- PRI拡張ボードのPRIポート1から5までをISDN回線で使用し、PRIポート6を高速ディジタル回線で使用している
- モデムユーザが2人（ユーザ名がvaio3とsalsa）とISDNユーザが1人（ユーザ名がjamyra）が接続中

の場合です。

(1) 「linestat -P」の表示例

```
# linestat -P
Mon Jan 15 14:49:07 JST 2001
<ISDN layer1/layer2 status>
            :
 1-1  layer1: F1(RUNNING)     layer2:ESTABLISH   (TEI:0)
 1-2  layer1: F1(RUNNING)     layer2:ESTABLISH   (TEI:0)
 1-3  layer1: F1(RUNNING)     layer2:ESTABLISH   (TEI:0)
 1-4  layer1: F1(RUNNING)     layer2:ESTABLISH   (TEI:0)
 1-5  layer1: F1(RUNNING)     layer2:ESTABLISH   (TEI:0)
 1-6  layer1: F1(RUNNING)
#
```

上記表示例では、PRIポート1から5のISDN回線とPRIポート6の高速ディジタル回線のレイヤ1が確立し、またISDN回線の場合DチャネルのLAPDが確立していることがわかります。

(2) 「linestat isdn」の表示例

```
# linestat isdn
Mon Jan 15 14:49:15 JST 2001
<ISDN status>
 PORT  CH  STATE                 TYPE    CONNECT-TIME    TELNO
  1-1  B1  enable :connect(In)   MODEM   01/15 14:28:43
    :
  1-1  B4  enable :connect(In)   HDLC    01/15 14:28:38  0474706013
    :
  1-1  B22 enable :connect(In)   MODEM   01/15 14:28:41
    :
#
```

この表示例では、ISDNの呼情報として

PRIポート1のB1チャネル　：モデムユーザが使用中
PRIポート1のB4チャネル　：ISDNユーザが使用中
PRIポート1のB22チャネル　：モデムユーザが使用中

であることがわかります。

(3) 「linestat isdn -s」の表示例

```
# linestat isdn -s
Mon Jan 15 14:49:19 JST 2001
<ISDN statistics>
 PORT    IN-CALL   IN-CONNECT      OUT-CALL  OUT-CONNECT    CHARGE
  1-1       2386         2381             0            0         0
  1-2       3933         3933             0            0         0
  1-3       6352         6351             0            0         0
  1-4         12           12             0            0         0
  1-5         34           34             0            0         0
  1-6          1            1             0            0         0
#
```

この表示内容から、各PRIポートにおいて、着信をした回数（IN-CALL）、着信してかつ着信を許可した回数（IN-CONNECT）がわかります。

(4) 「modemstat」の表示例

```
# modemstat
Mon Jan 15 14:49:34 JST 2001
<DigitalModem & Piafs status>
NO PORT  CH  STATE       CARRIER  R-RATE T-RATE  PROTOCOL COMP
1   1-1  B1  CONN        V34      31200  33600   LAPM     V42BIS
      :
10 ----  --  ----------  ------   -----  -----   -------  ------
      :
22  1-1  B22 CONN        V90      28800  49333   LAPM     V42BIS
      :
#
```

この表示内容から、モデム接続しているユーザが使用しているPRIポート、Bチャネル、および使用している通信規格（CARRIER）送信速度（T-RATE）などがわかります。

(5) 「linestat」の表示例

```
# linestat
Mon Jan 15 14:49:42 JST 2001
<PPP over ISDN status>
 INTERFACE  STATE    PROTOCOL  PORT  CH   CONNECT-TIME    USER-NAME
   :
 ncp66      connect   PPP       1-1  B1   01/15 14:29:05  vaio3
 ncp67      connect   PPP       1-1  B4   01/15 14:29:05  jamyra
 ncp68      connect   PPP       1-1  B22  01/15 14:29:02  salsa
<PPP over HSD status>
 INTERFACE  STATE    PROTOCOL  PORT  CH   CONNECT-TIME    USER-NAME
 hsd1       connect   PPP       1-6   1   01/04 09:10:58
#
```

この表示例から、

ユーザvaio3　：論理インタフェースncp66を使用してPPPで接続中
（拡張ボードスロット1-PRIポート1のB1チャネルを使用）
ユーザjamyra　：論理インタフェースncp67を使用してPPPで接続中
（拡張ボードスロット1-PRIポート1のB4チャネルを使用）
ユーザsalsa　：論理インタフェースncp68を使用してPPPで接続中
（拡張ボードスロット1-PRIポート1のB22チャネルを使用）

拡張ボードスロット1-PRIポート6を高速ディジタル回線で接続中であることがわかります。
また「linestat isdn」コマンドを実行し、同じPRIポート／Bチャネルが表示されている行をさがすことによって，各ユーザがモデム／ISDNのどちらで接続しているかわかります。
同様に「modemstat」コマンドを実行し、同じPRIポート／Bチャネルが表示されている行をさがすことによって、モデムで接続している場合の接続情報がわかります。

(6) 「netstat -r」の表示例

```
# netstat -r
 ROUTING TABLE
 destination       mask     gateway        if     property         cost
     :
*192.168.200.151  ffffffff                ncp66  -----               -
*172.31.11.18     ffffffff                ncp67  -----               -
*192.168.200.154  ffffffff                ncp68  -----               -
 133.30.0.1       ffffffff                hsd1   p-to-p              -
 0.0.0.0          00000000 172.31.11.111  en0    -----               3
 192.168.200.0    ffffff00                en1    direct              -
 172.31.0.0       ffff0000                en0    direct              -
 0.0.0.0          00000000                ipnhr0 unnumbered          -
 127.0.0.2        ffffffff                sink0  p-to-p,unnumbered   -
 172.31.2.241     ffffffff                lo0    p-to-p,loop         -
 127.0.0.1        ffffffff                lo0    p-to-p,loop         -
#
```

この表示例から、

論理インタフェースncp66　：　相手IPアドレス192.168.200.151
論理インタフェースncp67　：　相手IPアドレス172.31.11.18
論理インタフェースncp68　：　相手IPアドレス192.168.200.154
論理インタフェースhsd1　：　相手IPアドレス133.30.0.1

であることがわかります。
また「linestat」コマンドを実行し、同じ論理インタフェースの行をさがすことによって、各論理インタフェースを使用しているユーザ名がわかります。

7.3.4　具体的な切り分け手順

ここでは、**図7-1**の構成で、本装置に接続する接続相手から発信し、本装置に接続した後、本装置を経由してネットワーク上の通信相手に通信する場合の、具体的な切り分け手順について説明します。
まず通信のトラブルが、どのフェーズで発生しているのか、特定する必要があります。ここでは以下の５つのフェーズに分けて説明します。
なお、高速ディジタル回線の切り分け手順は、フェーズ①のPRI拡張ボードのチェック項目(**表7-4**の番号1から3)を確認後、フェーズ②を飛ばして③から順に行ってください。

フェーズ①：ISDN回線経由で、本装置に着信し、接続できているか。
フェーズ②：接続相手がモデムを使用して接続する場合、モデムが接続できているか。
フェーズ③：PPP接続／認証が成功しているか。
フェーズ④：本装置と同一セグメントにあるホストと通信できるか。
フェーズ⑤：本装置を経由してネットワーク上の通信相手と通信できるか。

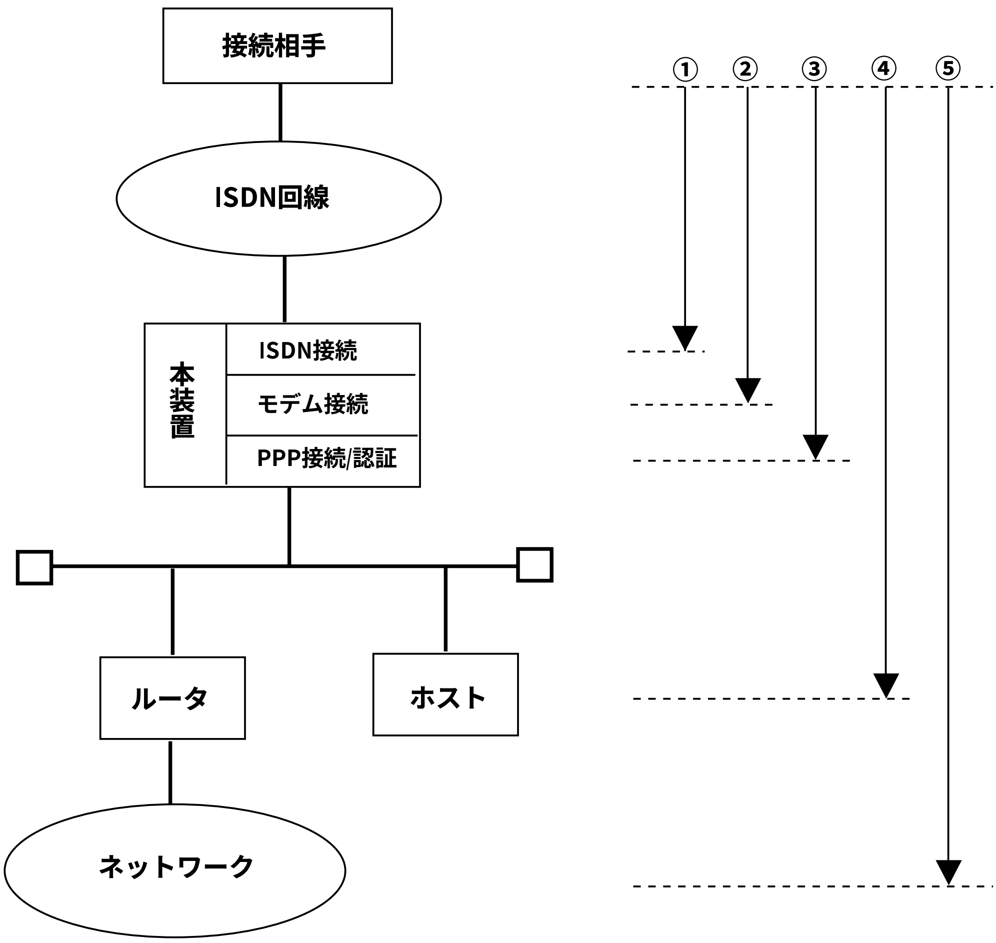


図7-1　通信機能のトラブルシューティングのフェーズ

フェーズ②は、接続相手がモデムの場合のみ有効です。またフェーズ④は、本装置と同一セグメント上にアクセスできるホストがある場合のみ有効です。

図7-1の各フェーズのどこまで通信できているかどうかの確認およびその対処について、**表7-3**に示します。各フェーズのチェック項目を実行し、その結果がOKにならない場合には、そのフェーズで何らかの障害、通信エラーが発生している可能性がありますので、その対処方法にしたがってトラブルの原因を切り分けてください。

表7-3　通信機能のトラブルのチェックポイントと対処方法

(1 / 2)

フェーズ	チェック項目	対処方法
①	接続相手の回線から電話機で本装置の電話番号に電話をかけてみてください。電話がつながりモデム音がきこえる場合には、本装置のISDN着信はOKです。	**(1)**項にしたがってチェックしてください。
②	接続相手から接続中に「modemstat」コマンドを実行し、STATEの表示がCONNになればOKです。	**(2)**項を参照してください。
③	接続相手から接続した時に、本装置の「linestat」コマンドを実行してください。 ISDN回線の場合は、接続相手のユーザ名が表示されていればOKです。 高速ディジタル回線の場合は、該当する論理インタフェース(hsd∗∗)のSTATEがconnectになればOKです。	**(3)**項にしたがってチェックしてください。
④	接続相手から本装置と同一セグメント上にあるホストにpingを実行してください。pingが成功すればOKです。　(*1)	・LANポートのケーブルの接続を確認してください。（**7.3.2**項参照） ・本装置のLANポートの設定（IPアドレス、ネットワークアドレスなど）が、接続しているネットワークに合っているか、正しく設定されているかを確認してください。（**4.5**項参照） ・本装置のフィルタが設定されている場合、フィルタが正しく設定されているか確認してください。（**4.6.1**項参照） ・接続相手のルーティング情報が正しく設定されているか確認してください。

表7-3　通信機能のトラブルのチェックポイントと対処方法

(2 / 2)

フェーズ	チェック項目	対処方法
⑤	接続相手からネットワーク上の通信相手にpingを実行してください。pingが成功すればOKです。 (*1)	・本装置のgatewaysファイルに、ネットワークへ到達するためのルーティング情報が正しく設定されているかを確認してください。（**4.5**項参照） ・本装置のフィルタが設定されている場合、フィルタが正しく設定されているか確認してください。（**4.6.1**項参照） ・接続相手において、ネットワークまでのルーティング情報が正しく設定されているか確認してください。

(*1)　通信相手にpingを行う場合には、応答が遅い場合がありますので、pingのtimeout時間（応答の待ち時間）を延ばして実行してみてください。またpingあるいはICMPのフレームに対してフィルタがかけられている場合がありますので、通信相手のホストがサポートしていると思われるプロトコル（HTTP、FTPなど）でも確認してみてください。

(1) 本装置にISDN接続が成功できない場合のチェック項目

この場合には、本装置のPRI回線に関する何らかのトラブルであると思われます。**表7-4**のチェック項目を確認してください。

表7-4　本装置にISDN接続が成功できない場合のチェック項目と対処方法

番号	チェック項目	対処方法
1	PRI拡張ボードのPRIランプが点灯していない。	PRI回線が使用可能な状態になっていません。PRIケーブルの接続、DSUの電源がONになっているかなどを確認してください。またPRIケーブルを抜いて、約10秒後に接続してから、何回か左記のコマンドを実行してください。それでも３が正常にならない場合には、回線提供業者にご相談ください。
2	「linestat -P」コマンドの結果、レイヤ1ステートがRUNNINGになっていない。	
3	「linestat -P」コマンドの結果、レイヤ1ステートがRUNNINGになっているが、レイヤ2ステートがESTABLISHになっていない。	
4	電話機を使用して、本装置に電話をかけても、接続できない。	本装置にISDN回線から着信していません。接続相手に設定されている接続先電話番号が正しいか確認してください。
5	接続相手から接続する前と、接続した後の「linestat isdn -s」コマンドを実行し、IN-CALLの統計が増えない。	
6	接続相手から接続する前と、接続した後の「linestat isdn -s」コマンドを実行し、IN-CALLの統計は増えるが、IN-CONNECTの統計が増えない。	本装置にISDNの着信は届いていますが、接続に失敗しています。 **付録B**の該当するWarningメッセージの表の対処方法を参照してください。
7	接続相手から接続すると、コンソールに付録Bの**表B-3～表B-10**に記述されているWarningメッセージが出力される。	

(2) 本装置にモデムで接続できない場合のチェック項目

モデムで本装置に接続する場合、モデムが接続されているアナログ回線、および本装置が接続されているISDN回線までの網内の回線品質の変動に影響を受ける場合があります。特に56Kモデムの場合、回線品質が悪い場合には接続できない場合があります。
何回か連続して接続できない場合には、時間帯を変えて接続してみてください。

TAのアナログポートにモデムを接続している場合には、そのTAのアナログポートの特性によっては、モデムが接続できない場合があります。この場合には、モデムを直接アナログ回線に接続してください。
またPBX経由で接続している場合にも、同様にモデムの接続性がよくない場合がありますので、モデムを直接アナログ回線に接続してください。

モデムから本装置に接続できない場合には、**表7-5**の対策を行うことによって、接続性が改善できる場合があります。

表7-5　モデムにおける接続性改善の対策

対　策	備　考
使用されているモデムのドライバ／ファームウェアを最新のバージョンにしてみてください。	特に、K56flexあるいはV.90の初期のモデムの場合には、接続性／安定性が向上する可能性があります。
モデムが接続されているアナログ回線に電話、モデム、FAXなどの機器が接続されている場合には、それらの機器をはずしてみてください。	――――
モデムのモジュラケーブルが極端に長い場合あるいは延長コネクタで延長している場合には、5m以内のケーブルで直接アナログ回線のモジュラジャックに接続してみてください。	――――
56Kモデムの接続性／安定性が悪い場合には、ATコマンドで接続MAX速度を、44000bps以下に設定してみてください。	MAX速度を低くすることで、接続性／安定性が改善できる場合があります。ただし44000bps程度であれば、実質的な転送速度が低下することはあまりありません。
56Kモデムの接続MAX速度を低くしても改善できない場合には、ATコマンドでV.34モードに固定して接続してみてください。	――――

(3) 本装置にPPP接続／認証が成功できない場合のチェック方法

PPP接続／認証で接続できない場合、PPPの接続手順、PPPの認証手順、またRADIUSサーバを使用している場合には、RADIUSサーバとの通信などにエラーが発生している可能性があります。

ISDN回線の場合は、まず以下の項目について確認してください。

- 本装置のusersファイルに設定されている認証方式が、接続相手の設定と合っているかどうか。（%presetのauth_requestの設定）
- 接続相手のパソコンあるいはルータに設定されているユーザ名／パスワードの設定が正しいかどうか。
- RADIUSサーバを使用している場合、本装置のradiusファイルの設定と、RADIUSサーバ側の設定内容が正しいかどうか。

また**表7-6**のチェック項目も、確認してください。
高速ディジタル回線の場合は、PPP接続に失敗している可能性があります。**表7-6**のチェック項目(番号1)を確認してください。

表7-6　本装置にPPP接続／認証が成功できない場合のチェック方法

番号	チェック項目	対処方法
1	本装置のコンソールにPPP関連のWarningメッセージ（**付録B**の**表B-11**、**表B-13〜表B-14**、**表B-16**）が出力される。	PPPの接続手順で何らかのエラーが発生しています。 付録Bの該当するWarningメッセージの表の対処方法を参照してください。
2	本装置のコンソールに、認証関連のWarningメッセージ（**付録B**の**表B-12**）が出力される。	PPPの認証手順で何らかのエラーが発生している可能性があります。接続相手の端末に設定されているユーザ名、パスワードを確認してください。また付録Bの該当するWarningメッセージの表の対処方法を参照してください。
3	本装置のコンソールに、RADIUS関連のWarningメッセージ（**付録B**の**表B-19**）が出力される。	RADIUSサーバとの通信で何らかのエラーが発生している可能性があります。付録Bの該当するWarningメッセージの表の対処方法を参照してください。 また**「付録C　RADIUSサーバについて」**も参照してください。

付録A

エディタの使い方

付録Aでは、ファイルの編集を行うエディタの使用方法を詳しく説明しています。

本章の内容

A.1　エディタの概要

エディタは、本装置のセットアップファイルを編集するものです。セットアップファイルを行単位で編集する簡易ラインエディタです。
編集機能としては、行の追加 / 削除 / 一部変更 / コピー / 移動 / 検索などの機能があります。

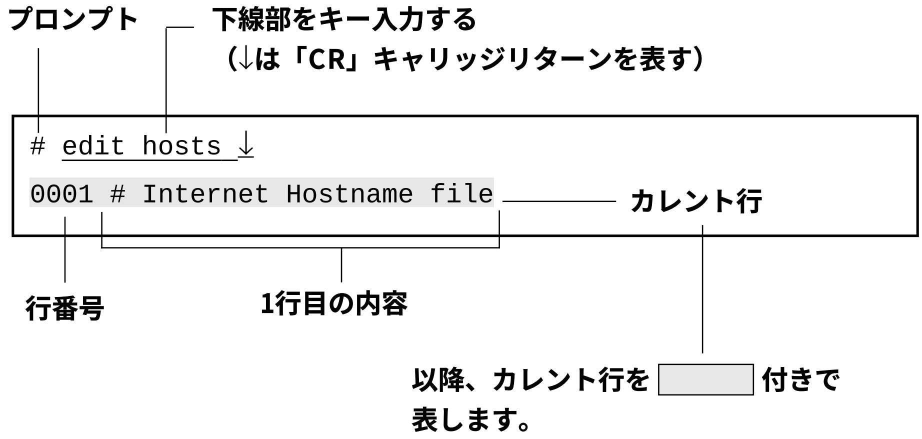
(1) 編集ファイルの表示

エディタで編集できるファイル名の一覧とその概要は、以下のようにして表示します。

```
# edit -h↓
# IP
   gateways      IP Static Gateway Information
   interface     IP Direct Attached segment Information
   hostname      My Host Name
   hosts         Host Name and its IP-address
   netmask       IP Subnet Mask
   ipfilters     IP Packet Filter
   resolv.conf   Domain Name System
   services      Service Name and Port Number
   snmpconf      SNMP Parameters
   rip.conf      RIP Configuration
   syslog.conf   SYSLOG Configuration
# WAN
   boards        Extension Board Configurations
   users         Remote User Configurations
   radius        RADIUS Server Parameters
   ippool        IP Pool Configurations
# ETC.
   servers       Server Programs
```

(2) エディタの起動

スーパーユーザのプロンプトが表示されている状態で、「edit ファイル名↓」と入力すると、エディタが起動します。編集モードになり、下図のように行番号とそのファイルの１行目が表示されます。編集モードではエディタのサブコマンドを使用してファイルの編集を行います。カレント行は、１行目になります。カレント行とは、現在、編集の対象となっている行のことです。



(3) サブコマンド

エディタのサブコマンドの一覧を**表A-1**に示します。各サブコマンドは1文字のコマンドで、その文字を入力した時点で実行されます。パラメータを必要とするサブコマンド（j や lコマンド) は、プロンプトを表示してパラメータの入力待ちになります。
各サブコマンドの詳細は、次節で説明します。

表A-1　サブコマンド一覧

分　類	コマンド	機　　能
カレント行の移動	n	次の行に移動する
	p	1つ前の行に移動する
	t	ファイルの先頭に移動する
	b	ファイルの最後に移動する
	j	指定した番号の行に移動する
行の追加	a	ファイルの最後に１行追加する
	o	カレント行の次に1行追加する
	i	カレント行の前に1行追加する
行の削除	d	カレント行を削除する
行の内容編集	c	カレント行の内容を編集する
行の内容表示	l	指定した範囲の行の内容を表示する
	<CR>	カレント行の内容を表示する
文字列の検索	s	指定した文字列を検索する
行のコピー	y	カレント行の内容を一時バッファに記憶する
	z	一時バッファの内容をカレント行の次に追加する
サブコマンド一覧表示	?	サブコマンドの一覧を表示する
エディタの終了	q	ファイルにセーブしないで終了する
	e	ファイルにセーブして終了する

A.2　エディタのサブコマンド

A.2.1　カレント行の移動

カレント行を移動するコマンドには以下のものがあります。

n　　-----　次の行に移動する
p　　-----　1つ前の行に移動する
t　　-----　ファイルの先頭に移動する
b　　-----　ファイルの最後に移動する
j　　-----　指定した番号の行に移動する

下図の例では、カレント行が４行目の「128.22.0.2　host2」の行にあるときに、それぞれのコマンド実行後のカレント行の位置を←で示しています。

行番号	ファイルの内容	
0001	# hostname file	← tコマンド実行後
0002	# 1994.8.12 updated	
0003	128.22.0.1 host1	← pコマンド実行後
0004	128.22.0.2 host2	（カレント行）
0005	128.22.5.1 pc1	← nコマンド実行後
0006	128.22.5.2 pc2	
0007	128.22.99.1 router1	
0008	128.22.99.2 router2	← jコマンド(8行目指定)実行後
0009	128.23.99.1 router_A1	
0010	# end of hostname file	← bコマンド実行後

(1) nコマンド

文字「n」を入力すると、カレント行が次の行に移動し、移動した行の内容が表示されます。
ファイルの最後で「n」を入力すると、[END]が表示され、カレント行はファイルの最後のままです。

```
0004  128.22.0.2    host2      （カレント行）
0005  128.22.5.1    pc1        ← nコマンド実行後
```

次の行の内容が表示される

```
0010  # end of hostname file   （カレント行）
[END]                          ← nコマンド実行後
```

ファイルの最後を示す。

(2) pコマンド

文字「p」を入力すると、カレント行が1つ前の行に移動します。
カレント行が１行目のときに「p」を入力すると、[TOP]が表示され、カレント行は１行目のままです。

```
0004  128.22.0.2    host2      （カレント行）
0003  128.22.0.1    host1      ← pコマンド実行後
```

1つ前の行の内容が表示される。

```
0001 # hostname file           （カレント行）
[TOP]                          ← pコマンド実行後
```

ファイルの先頭を示す。

(3) tコマンド

文字「t」を入力すると、カレント行が１行目（ファイルの先頭）に移動します。

```
0004  128.22.0.2    host2      （カレント行）
0001  #  hostname file         ← tコマンド実行後
```

先頭の行の内容が表示される。

(4) bコマンド

文字「b」を入力すると、カレント行がファイルの最後に移動します。

```
0004  128.22.0.2    host2               （カレント行）
0010  # end of hostname file            ← bコマンド実行後
```

最後の行の内容が表示される。

(5) jコマンド

文字「j」を入力すると、カレント行が指定した番号の行に移動します。

```
0004  128.22.0.2    host2               （カレント行）
jump> 8↓                                ← jコマンド入力
0008  128.22.99.2   router2             ← 8行目指定後
```

プロンプト「jump>」が表示されるので移動先の行番号を入力する。
指定した８行目の内容が表示される。

```
0004  128.22.0.2    host2               （カレント行）
jump> 888↓                              ← jコマンド入力
out of range.                           ← 888行目指定
```

指定した行が存在しない場合には、「out of range」メッセージが表示され、
カレント行は４行目のままである。

付録 エディタの使い方

A.2.2　行の追加

行を追加するコマンドには以下のものがあります。

a　　-----　ファイルの最後に1行追加する
o　　-----　カレント行の次に1行追加する
i　　-----　カレント行の前に1行追加する

下図の例では、カレント行が４行目の「128.22.0.2　host2」の行にあるときに、それぞれのコマンドで行が追加される位置を←で示しています。

行番号	ファイルの内容	
0001	# hostname file	
0002	# 1994.8.12 updated	
0003	128.22.0.1 host1	←iコマンド
0004	128.22.0.2 host2	（カレント行）
0005	128.22.5.1 pc1	←oコマンド
0006	128.22.5.2 pc2	
0007	128.22.99.1 router1	
0008	128.22.99.2 router2	
0009	128.23.99.1 router_A1	
0010	# end of hostname file	
0011		←aコマンド

(1) aコマンド

aコマンドはファイルの最後に1行追加するコマンドです。文字「a」を入力すると、これから追加する行番号と文字「<」が表示され、行入力モードになります。ここで、追加する行を入力してください。行の入力の終了は、キャリッジリターンです。キャリッジリターンを入力すると追加した行が再表示されます。
追加後のカレント行は、ファイルの最後の行（追加した行）になります。

```
0004  128.22.0.2    host2
0011< 128.23.99.2   router_A2 ↓
0011  128.23.99.2   router_A2
```

（カレント行）
← aコマンド入力後
追加する行番号
追加する行を入力する。

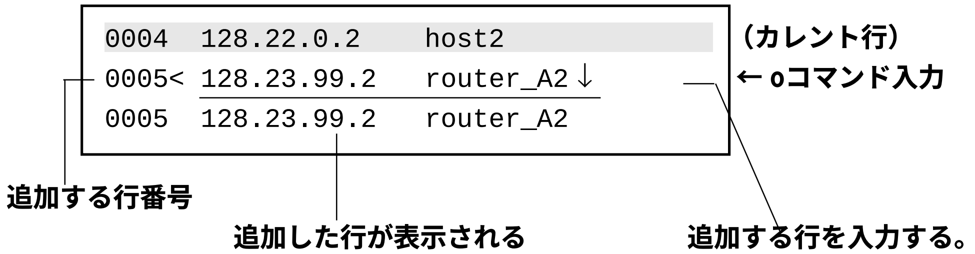
行入力モード

行入力モードでは、入力した文字がカーソルの前に追加されます。もし、入力中に打ち間違いをした場合には、「BS」または「DEL」キーで１文字ずつ消去して打ち直してください。
すでに入力した文字の一部を修正したい場合には、「^b」（CTRLキーを押したままbキーを押す）でカーソルを１文字ずつ戻したり、「^f」（CTRLキーを押したままfキーを押す）でカーソルを1文字ずつ進めたり、「^t」(CTRLキーを押したままtキーを押す)でカーソルを先頭に戻したりできます。カーソルを修正したい位置に移動して、「BS」または「DEL」キーで誤った文字を消去したり、新たな文字を追加入力することもできます。
行の入力自身をキャンセルしたい場合には「ESC」キーを入力します。「ESC」キーを入力すると行入力モードが終了して、もとのカレント行が表示されます

BS ----- カーソルの前の１文字を消去する
DEL ----- カーソルの１文字を消去する
^b ----- カーソルを１文字戻す
^f ----- カーソルを１文字進める
^t ----- カーソルを先頭に戻す
ESC ----- 行入力モードをキャンセルする

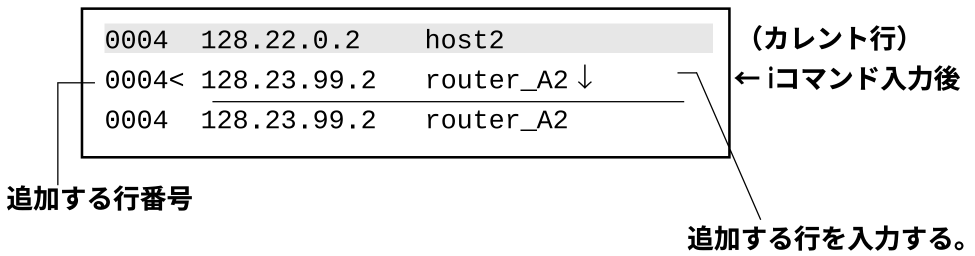
(2) oコマンド

oコマンドは、カレント行の次に1行追加するコマンドです。文字「o」を入力すると、これから追加する行番号と文字「<」が表示され、行入力モードになります。ここで、追加する行を入力してください。行の入力の終了は、キャリッジリターンです。キャリッジリターンを入力すると追加した行が再表示されます。
追加後のカレント行は、次の行（追加した行）になります。追加した行の後ろの行は、行番号が増えて1つずつ後ろにずれます。



(3) iコマンド

iコマンドは、カレント行の前に1行追加するコマンドです。文字「i」を入力すると、これから追加する行番号と文字「<」が表示され、行入力モードになります。ここで、追加する行を入力してください。行の入力の終了は、キャリッジリターンです。キャリッジリターンを入力すると追加した行が再表示されます。
追加後のカレント行は、元のカレント行と同じ行番号（追加した行）になります。
元のカレント行から後ろの行は、行番号が増えて1つずつ後ろにずれます。



A.2.3　行の削除

(1) dコマンド

dコマンドは、行の削除をするコマンドです。文字「d」を入力すると、カレント行が削除され、次の行が表示されます。
削除後のカレント行は、削除した次の行（ただし、1行削除されているのでカレント行の番号は変わりません）になります。

```
0004  128.22.0.2    host2
0004  128.22.5.1    pc1
```

（カレント行）
← dコマンド実行後

次の行が表示される

```
0010  # end of hostname file
1 line deleted.
[END]
```

（カレント行）
← dコマンド実行後

ファイルの終了を示す

付録　エディタの使い方

A.2.4　行の内容編集

(1) cコマンド

cコマンドはカレント行の内容を編集するコマンドです。文字「c」を入力すると、編集する行番号と文字「>」に続いて編集前の内容が表示され、次に行番号と文字「<」が表示され、行編集モードになります。ここで、新規に行を入力するか、「^u」を入力して元の行を編集してください。行の編集の終了は、キャリッジリターンです。キャリッジリターンを入力すると編集した行が再表示されます。
編集後のカレント行は、変わりません（すなわち、編集した行になります）。

変更内容を新規に入力する場合

```
0004  128.22.0.2    host2
0004> 128.22.0.2    host2
0004< 128.22.0.2    host_A2↓
0004  128.22.0.2    host_A2
```

（カレント行）
←cコマンド入力

変更された内容が表示される

変更する内容を新規に入力する

一部を変更する場合

```
0004  128.22.0.2    host2
0004> 128.22.0.2    host2
0004< 128.22.0.2    host□
```

（カレント行）
←cコマンド入力

「^u」を入力すると元の内容が表示されるので、
「BS」を入力して１文字消去する

```
0004  128.22.0.2    host2
0004> 128.22.0.2    host2
0004< 128.22.0.2    host_A2↓
0004  128.22.0.2    host_A2
```

（カレント行）
←cコマンド入力

「_A2」とキャリッジリターンを入力する

行編集モード

行編集モードでは、「^u」（CTRLキーを押したままuキーを押す）を入力すると編集中の行バッファは元の行の内容になる点が、行入力モードと異なります。その他の操作は行入力モードと同じです。

行編集モードでは、入力した文字がカーソルの前に追加されます。もし、入力中に打ち間違いをした場合には、「BS」または「DEL」キーで１文字ずつ消去して打ち直してください。

すでに入力した文字の一部を修正したい場合には、「^b」（CTRLキーを押したままbキーを押す）でカーソルを１文字ずつ戻したり、「^f」（CTRLキーを押したままfキーを押す）でカーソルを1文字ずつ進めたり、「^t」(CTRLキーを押したままtキーを押す)でカーソルを先頭に戻したりできます。カーソルを修正したい位置に移動して、「BS」または「DEL」キーで誤った文字を消去したり、新たな文字を追加入力することもできます。

行の入力自身をキャンセルしたい場合には「ESC」キーを入力します。

BS ----- カーソルの前の１文字を消去する
DEL ----- カーソルの１文字を消去する
^b ----- カーソルを１文字戻す
^f ----- カーソルを１文字進める
^t ----- カーソルを先頭に戻す
^u ----- 行バッファを元の行の内容にする
ESC ----- 入力モードをキャンセルする

A.2.5　行の内容表示

(1) lコマンド

lコマンドは、指定した範囲の行を表示するコマンドです。文字「l」を入力すると、プロンプト「line」が表示され、表示範囲の入力待ちになります。表示したい行番号を入力すると、その行の内容が表示されます。
表示後のカレント行は、変わりません。
表示範囲の指定は、2行目から10行目を表示したい場合には「2,10」と指定します。４行目のみを指定したい場合には、「4」と指定します。

```
0004  128.22.0.2    host2
line> 2,6↓
0002  #  1994.8.12 updated
0003  128.22.0.1    host1
0004* 128.22.0.2    host2
0005  128.22.5.1    pc1
0006  128.22.5.2    pc2
```

（カレント行）
← lコマンド入力
表示する行番号を入力する
カレント行には「*」が付く

(2) キャリッジリターン

サブコマンド入力状態でキャリッジリターンのみを入力すると、カレント行の内容が表示されます。カレント行は、変わりません。

```
0004  128.22.0.2    host2
0004  128.22.0.2    host2
```

（カレント行）
←キャリッジリターン入力

A.2.6　文字列の検索

(1) sコマンド

sコマンドは、指定した文字列を検索するコマンドです。文字「s」を入力すると、プロンプト「search」が表示され、検索文字列の入力待ちになります。検索したい文字列を入力すると、カレント行の次の行から文字列の検索が行われます。
指定した文字列を含む行があれば、カレント行はその行になります。一方、指定した文字列を含む行がなかった場合には、カレント行は変わりません。
検索文字列にキャリッジリターンのみを入力すると、直前のsコマンドで指定した検索文字列が検索されます。

```
0004  128.22.0.2    host2          （カレント行）
search> route_A1↓                  ← sコマンド入力
0009  128.23.99.1   router_A1      検索する文字列を入力する
```

指定した文字列を含む行が表示され、この行がカレント行になる

```
0004  128.22.0.2    host2          （カレント行）
search> route_A1↓                  ← sコマンド入力
search string not found.           検索する文字列を入力する
```

指定した文字列を含む行がなかった場合には、このメッセージが表示されて、カレント行は元のままである。

A.2.7　行のコピー

(1) yコマンド

yコマンドは、カレント行の内容を一時バッファに記憶するコマンドです。カレント行の内容は変わりません。zコマンドと組み合わせて使うことにより、行のコピーを行います。カレント行は変わりません。

注意　　**一時バッファに記憶するコマンドは、yコマンドの他にdコマンドがあります。**

注意　　**一時バッファに記憶できるのは１行だけです。yコマンド / dコマンドを実行すると、以前に記憶されていた一時バッファの内容は失われてしまいます。**

```
0004  128.22.0.2    host2
1 line (0004) stored.
```

（カレント行）
← yコマンド入力
記憶された行番号が表示される

(2) zコマンド

zコマンドは、一時バッファに記憶されている内容をカレント行の次に追加するコマンドです。zコマンドを実行すると、追加する行が表示され、その行の編集モードになります。キャリッジリターンを入力して、行の編集を終了するとカレント行は追加した行になります。
行編集モードについては、「**A.2.2　行の追加**」を参照してください。

```
0004  128.22.0.2    host2
0005< 128.22.0.1    host1
```

（カレント行）
← zコマンド入力
追加する行番号
一時バッファの内容がコピーされ、行編集モードになる

[行をコピーする手順]

① コピーする行に移動します。
② yコマンドで一時バッファにその行を記憶します。
③ コピー先の行に移動します（移動した次の行にコピーされます）。
④ zコマンドで記憶した行を追加します。

[行をムーブする手順]

① ムーブする行に移動します。
② dコマンドでその行を削除します（削除した行は一時バッファに記憶されます）。
③ ムーブ先の行に移動します（移動した次の行にコピーされます）。
④ zコマンドで記憶した行を追加します。

A.2.8　サブコマンド一覧の表示

(1) ?コマンド

?コマンドは、エディタのサブコマンド一覧を表示するコマンドです。文字「?」を入力すると、エディタのサブコマンド一覧、行入力モード / 行編集モードのコマンドと現在編集中のファイル名が表示されます。

「?」を入力

```
+----<edit commands>-----------------------------+
| t: top line                b: bottom line      |
| n: next line               l: list             |
| p: previous line           s: search strin     |
| d: delete line             o: append line      |
| c: change line             y: store line       |
| a: add line                z: recover lin      |
| i: insert line             j: jump line        |
| q: quit                    e: exit             |
+----<column edit commands>----------------------+
| ^f: 1 column right         ^b: 1 column left   |
| ^t: top column                                 |
| ^u: recover column(1 line)                     |
+----<edit file name>----------------------------+
| hosts                                          |
+------------------------------------------------+
```

現在編集中のファイル名が表示される

付録　エディタの使い方

A.2.9　エディタの終了

(1) qコマンド

qコマンドは、編集した内容をファイルにセーブしないで、エディタを終了するコマンドです。文字「q」を入力すると、現在編集中のファイルに対する変更内容はすべて放棄され、ファイルはもとのままです。

ファイルが変更されている場合

```
0004  128.22.0.2    host2            （カレント行）
file is modified. really quit ?      ← qコマンド入力
```

ファイルが変更されている場合には、確認メッセージが表示される。
「y」を入力すると編集内容は放棄されて、エディタを終了する。
「y」以外の文字を入力すると、サブコマンド入力待ちになる。

ファイルが変更されていない場合

```
0004  128.22.0.2    host2            （カレント行）
#                                    ← qコマンド入力
```

ファイルが変更されていない場合には、エディタは終了してコマンドインタプリタに戻る。

(2) eコマンド

eコマンドは、編集した内容をファイルにセーブして、エディタを終了するコマンドです。文字「e」を入力すると、現在編集中のファイルが更新されます。

注意　**セーブした内容はメモリ上の一時ファイルに書かれます。セットアップカードに保存するにはwriteコマンドを実行してください。writeコマンドを実行しないで、電源をオフにしたり、リブートしたりすると変更内容が失われてしまいます。**

```
0004  128.22.0.2    host2            （カレント行）
#                                    ← eコマンド入力
```

エディタは終了してコマンドインタプリタに戻る。

付録B
コンソールおよびsyslogに出力されるメッセージ一覧

ここでは、本装置のコンソールおよびsyslogに出力されるメッセージの種類と意味について説明します。
各コマンド実行時に表示されるエラーメッセージについては、「6章　コマンドの説明」を参照してください。

本章の内容

B.1　エラーメッセージの表示方法

エラーメッセージは、本装置のCONSOLEポートに接続した端末に自動的に表示されます。RS-232Cインタフェースを持った端末やVT端末エミュレータを搭載したパソコンを、CONSOLEポートに接続してエラーメッセージを確認できます。
また、IPネットワークでは本装置はTELNETサーバ機能を持っていますので、ネットワーク上のUNIXワークステーションなどからtelnetクライアントで本装置にログインして、consoleコマンドを実行するとコンソールに表示されるエラーメッセージを確認することができます(6章のconsoleコマンド参照)。
さらに本装置のsyslog機能をonにすることによって、エラーメッセージをあらかじめ設定されているホストにsyslogメッセージとして出力することができます。

B.2　エラーメッセージの見方

(1) Warning (ウォーニング) メッセージ

Warningメッセージは、エラーの発生や状態変化およびセットアップ内容のエラーを表示するメッセージです。
このメッセージは通信の障害が発生したときに、障害の原因や障害箇所の切り分けに役立つものです。
Warningメッセージが表示されていても、それが通信障害の原因を示す場合と、一時的な障害を示す場合と、単なる情報を表示する場合があります。
また、1つの障害に対して複数のWarningメッセージが表示される場合もあります。障害の発生時には、そのメッセージが発生した時刻をもとに、前後のメッセージも参照するようにしてください。

注 意　**Warningメッセージが表示されていても、一時的なエラーの表示で、すでに回復している場合や単なる情報を表示している場合もあります。Warningメッセージについて対処が必要かどうかは、**

・現在、通信エラーなどの障害が発生しているか？
・Warningメッセージが発生した時刻
・各Warningメッセージの対処方法
・Warningメッセージの発生頻度

などを考慮してください。

(2) 本装置のコンソールに出力されるWarningメッセージのフォーマット

本装置のコンソールに出力されるWarningメッセージには、主に以下の２つのフォーマットがあります。

●Warningメッセージ表示例1

これは、主に通信中に発生した現象を表示する場合に使用されます。

```
@W(3/21 20:6:32):[CID 4018]:LCP(C1-4-20):abc:Echo-Fail(Retry-Out)
```

日付と時刻　**CID**　**分類**　**メッセージ**

日付と時刻

： 現象が発生した日付と時刻を表示します。メッセージによっては表示されないものもあります。

CID

： ISDN回線を使用した場合は、通信の開始から終了までの間で関連する複数のモジュールに渡ってユニークになるIDが表示されます。
分類が、CC、L2MUX、LCP、authd、MPs、BACP、BAP、ncpd、NCP、CBCPおよびDSPCの場合に表示されます。
高速ディジタル回線を使用した場合は、以下のように表示されます。
分類が、LCP、MPs、BACP、BAP、ncpd、NCPの場合に表示されます。

[CID xyyy]

x	：高速ディジタル回線で使用しているPRIボードのPRIポート番号(1〜6)
yyy	：PRIポート内の論理チャネル番号(001〜024) boardsファイルの%channelで設定した論理チャネル番号

分類

： 現象を検出したモジュールと識別情報が表示されます。

メッセージ

： それぞれの現象に対応したメッセージが表示されます。

●Warningメッセージ表示例2

これは、主にセットアップファイルの解析を行った場合に使用されます。

```
users(line X):inval keyword
```

行　**メッセージ**

行

： セットアップファイルの行番号が表示されます。

メッセージ

： それぞれの現象に対応したメッセージが表示されます。

表B-1に示す分類に従って、対応する表を参照してください。

(3) syslogで出力されるWarningメッセージのフォーマット

syslogに出力されるWarningメッセージは、本装置のコンソールに出力されるWarningメッセージの中の、主に通信中に発生した現象に関するWarningメッセージです。
本装置からsyslogメッセージを受信したホストにおける表示は、そのホストのsyslogの仕様に依存しますが、一般的には、以下のようなフォーマットで表示されます。

```
Aug 24 19:15:28  ns241 [CID 4018]:LCP(C1-4-20):abc:Echo-Fail(Retry-Out)
```

(A)　**CID**　**分類**　**メッセージ**

(A)

： この部分は、syslogメッセージを受信したホストが挿入します。

CID

： ISDN回線を使用した場合は、通信の開始から終了までの間で関連する複数のモジュールに渡ってユニークになるIDが表示されます。
分類が、CC、L2MUX、LCP、authd、MPs、BACP、BAP、ncpd、NCP、CBCPおよびDSPCの場合に表示されます。
高速ディジタル回線を使用した場合は、以下ののように表示されます。
分類が、LCP、MPs、BACP、BAP、ncpd、NCPの場合に表示されます。

[CID xyyy]

x　：高速ディジタル回線で使用しているPRIボードのPRIポート番号(1～6)
yyy　：PRIポート内の論理チャネル番号(001～024)
　　boardsファイルの%channelで設定した論理チャネル番号

分類

： 現象を検出したモジュールと識別情報が表示されます。

メッセージ

： それぞれの現象に対応したメッセージが表示されます。

表示されたメッセージは、**表B-1**に示す分類に従って、対応する表を参照してください。
ただし、syslogに出力されるのは、主に通信中に発生した現象に関するWarningメッセージですので、**表B-1**に記述されている中の、**表B-2**～**表B-21**に関するwarningメッセージのみです。

表B-1　Warningメッセージの分類と対応表

分類	参照表	Warningメッセージが出力される主な状況
EN	**表B-2**	イーサネットの通信
L2ME, LAPD	**表B-3**	ISDNのlayer2の通信
CC, L2MUX, CCMUX	**表B-4～表B-10**	ISDNの呼制御処理
LCP	**表B-11**	PPPのLCP接続/切断処理
authd	**表B-12**	PPPの認証手順
MPs	**表B-13**	PPPおよびMPの接続処理
BACP	**表B-14**	BACPの接続／切断処理
BAP	**表B-15**	BAPのリンク追加／リンク削除処理
ncpd/NCP	**表B-16**	PPPのIPCP接続/切断処理
isdncb	**表B-17**	無課金コールバック
CBCP	**表B-18**	CBCPコールバック
radiusd, acctd	**表B-19**	RADIUSサーバとの通信
RADIUSserver	**表B-20**	RADIUS認証サーバの認証結果の解析
snmpd	**表B-21**	SNMPの動作
routed	**表B-22**	RIPの動作
DSPC	**表B-23**	DSPにおけるモデム／PIAFSの接続処理
boards	**表B-24**	boardsファイルの解析
users	**表B-25**	usersファイルの解析
radius	**表B-26**	radiusファイルの解析
ippool	**表B-27**	ippoolファイルの解析
interface	**表B-28**	interfaceファイルの解析
gateways	**表B-29**	gatewaysファイルの解析
snmpd:snmpconf	**表B-30**	snmpconfファイルの解析
rip.conf	**表B-31**	rip.confファイルの解析
syslog.conf	**表B-32**	syslog.confファイルの解析

注 意　**表B-1に記述されている参照表のうち、表B-24以降のWarningメッセージはsyslogには出力されません。**

B.3　メッセージ一覧

■ EN Warningメッセージ

これは、イーサネットの通信に関するWarningメッセージです。

表B-2　Warningメッセージ一覧(EN)

メッセージ	意　味	対　処
EN: duplicated proto address sent from X	自局IPアドレスと同じIPアドレスのARPフレームを、MACアドレスXから受信した。	hostsファイルに設定した本装置のIPアドレスを確認してください。また、同じIPアドレスが他の装置に設定されていないか確認してください。
enFCC(0, X): LINK lost (cable problem?)	イーサネットのキャリアを検出できなかった。 (X=0：LAN1ポート) (X=2：LAN2ポート)	LANポートのケーブルの接続を確認してください。
enFCC(0, X): Parallel detection fault	ハブとのネゴが失敗した。 (X=0：LAN1ポート) (X=2：LAN2ポート)	interfaceファイルのphyサブキーワードでハブと同一のスピードを設定してください。
enFCC(0, X): Remote (HUB) fault	ハブから故障している信号を受信した。 (X=0：LAN1ポート) (X=2：LAN2ポート)	ハブの状態等を確認してください。

■ L2ME/LAPD Warningメッセージ

これは、ISDN回線のlayer2の通信に関するWarningメッセージです。

表B-3　Warningメッセージ一覧(L2ME/LAPD)

メッセージ	意　味	対　処
L2ME: ID-REQ Retryout	lapd設定のためのTEI値の要求を網に送信したがretryoutした。	このエラーが発生しても通信に支障が無い場合には、特に対処する必要はありません。 通信障害が発生している場合には、本装置とDSU間のケーブルの接続や接触を確認してください。それでも回復しない場合には、交換機とDSU間の接続を回線提供業者に確認を依頼してください。
L2ME: ID-REQ Rejected	lapd設定のためのTEI値の要求を網に送信したが網に拒否された。	
LAPD:Px-y(0):Status(X)	lapdにおいてなんらかのイリーガルなstatus(X：内部コード)が発生した。	

■ CC／L2MUX／CCMUX Warningメッセージ

これは、主にISDN回線の接続、発呼、着呼に関連するWarningメッセージです。
次のようなフォーマットになっています。

［CC Warningメッセージのフォーマット］

[CID ****]:CC:Px-y:OutFail(P1,P2,P3,P4)
[CID ****]:CC:Px-y:InFail(P1,P2,P3,P4)
[CID ****]:CC:Px-y:DiscInd(P1,P2,P3,PCH,P4)
[CID ****]:CC:Px-y:メッセージ

Px-y：PRIボードのスロット番号／ポート番号

x　：発着信したPRIボードのスロット番号
y　：発着信したPRIボードのPRIポート番号

P1：回線サービス種別

CS　：回線交換(HDLC接続)
CS[PIAFS(V1.0)]　：回線交換(PIAFS(V1.0)接続)
CS[PIAFS(V2.0)]　：回線交換(PIAFS(V2.0)接続)
CS[PIAFS(V2.1)]　：回線交換(PIAFS(V2.1)接続)
CS[MODEM]　：回線交換(モデム接続)

P2：呼番号

P3：相手電話番号

：サブアドレスがある場合は、*(アスタリスク)で区切られた後に表示されます。

P4：詳細メッセージ

：状況を示すメッセージが表示されます。
さらに網側から切断された場合に限り、詳細メッセージの後ろに通知された理由表示が以下のフォーマットで表示されます。
(#<理由表示値>,<生成源>)
また理由表示値の後に、角括弧で付加情報が表示される場合もあります。
生成源には、この理由表示を生成した場所が表示されます。

0：ユーザ	1：自局私設網	2：自局公衆網
3：中継網	4：相手局公衆網	5：相手局私設網
7：国際網	10：インターネットワーキング先の網	

PCH：物理チャネル

：ISDNのチャネル番号が、B1などのように表示されます。

［L2MUX Warningメッセージのフォーマット］

[CID ****]:L2MUX:Px-y:OutFail(P1,P2,P3)
[CID ****]:L2MUX:Px-y:InFail(P1,P2,P3)

Px-y：PRIボードのスロット番号／ポート番号

x	：発着信したPRIボードのスロット番号
y	：発着信したPRIボードのPRIポート番号

P1：回線サービス種別

CS	：回線交換(HDLC接続)
CS[PIAFS(V1.0)]	：回線交換(PIAFS(V1.0)接続)
CS[PIAFS(V2.0)]	：回線交換(PIAFS(V2.0)接続)
CS[PIAFS(V2.1)]	：回線交換(PIAFS(V2.1)接続)
CS[MODEM]	：回線交換(モデム接続)

P2：相手電話番号

： サブアドレスがある場合は、*(アスタリスク)で区切られた後に表示されます。

P3：詳細メッセージ

： 状況を示すメッセージが表示されます。

［CCMUX Warningメッセージのフォーマット］

[CID ****]:CCMUX:Px-y:OutFail(P1,P2,P3)
[CID ****]:CCMUX:Px-y:InFail(P1,P2,P3)

Px-y：PRIボードのスロット番号／ポート番号

x	：発着信したPRIボードのスロット番号
y	：発着信したPRIボードのPRIポート番号

P1：回線サービス種別

CS	：回線交換(HDLC接続)
CS[PIAFS(V1.0)]	：回線交換(PIAFS(V1.0)接続)
CS[PIAFS(V2.0)]	：回線交換(PIAFS(V2.0)接続)
CS[PIAFS(V2.1)]	：回線交換(PIAFS(V2.1)接続)
CS[MODEM]	：回線交換(モデム接続)

P2：相手電話番号

： サブアドレスがある場合は、*(アスタリスク)で区切られた後に表示されます。

P3：詳細メッセージ

： 状況を示すメッセージが表示されます。

表B-4　Warningメッセージ一覧(CC/L2MUX/CCMUX)

メッセージ	意　味	対　処
CC:Px-y:OutFail(...)	ISDN回線で発呼に失敗した。	ダイヤルした相手電話番号(P3)を確認してください。対処については詳細メッセージ(P4)から**「表B-5　CC:OutFailの詳細メッセージの意味と対処」**をご覧ください。
CC:Px-y:InFail(...)	ISDN回線で着呼したが、本装置が拒否したか、その他の理由で接続に失敗した。	発信元電話番号(P3)を確認してください。対処については詳細メッセージ(P4)から**「表B-8　CC:InFailの詳細メッセージの意味と対処」**をご覧ください。
CC:Px-y:STATUS(...)->	状態表示(STATUS)メッセージを送信した。	特に対処は必要ありません。
CC:Px-y:<-STATUS(...)	状態表示(STATUS)メッセージを受信した。	このPRIポートの自局電話番号の設定を確認してください。
CC:Px-y:<-REST(...)	初期設定(RESTART)メッセージを受信した。	特に対処は必要ありません。
CC:Px-y:RESTACK(...)->	初期設定確認(RESTART ACKNOWLEDGE)メッセージを送信した。	特に対処は必要ありません。
CC:Px-y:DiscInd(...)	ISDN回線が通信中に異常な原因で切断された。	このメッセージが頻繁に出力され、通信障害が続く場合は、回線提供事業者、弊社サービス拠点、弊社代理店のいずれかまで連絡してください。
L2MUX:Px-y:OutFail(...)	ISDN回線で発呼に失敗した。	ダイヤルした相手電話番号(P2)を確認してください。対処については詳細メッセージ(P3)から**「表B-6　L2MUX:OutFailの詳細メッセージの意味と対処」**をご覧ください。
L2MUX:Px-y:InFail(...)	ISDN回線で着呼したが、本装置が拒否したか、その他の理由で接続に失敗した。	発信元電話番号(P2)を確認してください。対処については詳細メッセージ(P3)から**「表B-9　L2MUX:InFailの詳細メッセージの意味と対処」**をご覧ください。
CCMUX:Px-y:OutFail(...)	ISDN回線での発呼に失敗した。	対処については**「表B-7　CCMUX:OutFailの詳細メッセージの意味と対処」**をご覧ください。
CCMUX:Px-y:InFail(...)	ISDN回線での着呼を拒否した。	対処については**「表B-10　CCMUX:InFailの詳細メッセージの意味と対処」**をご覧ください。

表B-5　CC:OutFailの詳細メッセージの意味と対処

(1 / 2)

詳細メッセージ	意　味	対　処
lapd/layer1 error	下位層で障害が発生した。	頻繁に発生する場合には、ケーブルの接続を確認してください。
redial prohibited	自動再発信回数の制限のため、発呼ができない。	約3分待ってから発呼してください。これ以前に出力されているCC:OutFailメッセージを参照してください。
not enable	このPRIポートがenable状態になっていない。	このPRIポートの設定(boardsファイル)がenableになっていることを確認してください。
no number(#1,<生成源>) no route for transit net(#2,<生成源>) no route for dest(#3,<生成源>)	ダイヤル番号が正しくない。	本装置に設定した相手電話番号を確認してください。
user busy(#17,<生成源>)	ダイヤル先の回線に空きチャネルがない。	ダイヤル先の回線に空きチャネルができるまでお待ちください。
no user resp(#18,<生成源>)	ダイヤル先の回線から応答がない。	ダイヤル先の装置が動作中で、回線に接続されていることを確認してください。
call rejected(#21,<生成源>)	ダイヤル先の装置に着呼を拒否された。	ダイヤル先の装置の設定を確認してください。
user break down(#27,<生成源>)	ダイヤル先の装置が故障中である。	ダイヤル先の装置が動作中で、回線に接続されていることを確認してください。
no channel(#34,<生成源>)	生成源が1,2の場合は、自分側の回線に空きチャネルがない。 生成源が0,4,5の場合は、ダイヤル先の回線に空きチャネルがない。	ダイヤル先の装置が動作中で、回線に接続されていることを確認してください。
net out of order(#38,<生成源>)	網(ISDN網)で障害が発生した。	頻繁に発生する場合は、各種ケーブルがしっかりと接続されていることを確認してください。それでも発生する場合は、回線提供業者にご相談ください。
net failure(#41,<生成源>)	網(ISDN網)で一時的な障害が発生している。	頻繁に発生する場合は、各種ケーブルがしっかりと接続されていることを確認してください。それでも発生する場合は、回線提供業者にご相談ください。

表B-5　CC:OutFailの詳細メッセージの意味と対処

(2 / 2)

詳細メッセージ	意　味	対　処
not member of CUG(#87,<生成源>)	ダイヤル先の回線は、グループセキュリティ機能を使用してアクセス制限を行っている。	本装置側の回線も相手と同一グループに属するように契約してください。
incompatible(#88,<生成源>)	ダイヤル先の回線に本装置と通信可能な端末は接続されていない。	ダイヤル先の回線に接続されている端末の種類を確認してください。
STATUS received	STATUSメッセージを通知されたため、発呼処理を中止した。	対処の必要はありません。
RESTART received	RESTARTメッセージを通知されたため、発呼処理を中止した。	対処の必要はありません。
T303 timeout T301 timeout T310 timeout	プロトコル上のタイムアウトが発生した。	対処の必要はありません。

表B-6　L2MUX:OutFailの詳細メッセージの意味と対処

詳細メッセージ	意　味	対　処
channel busy	内部チャネルリソースがビジーであるか、網指定チャネルがすでに使用中である。	内部チャネルリソースが空くまでお待ちください。
not enable	このPRIポートがenable状態になっていない。	このPRIポートの設定(boardsファイル)がenableになっていることを確認してください。

表B-7　CCMUX:OutFailの詳細メッセージの意味と対処

詳細メッセージ	意　味	対　処
channel busy	Bチャネルのリソースが確保できない。	内部チャネルリソースが空くまでお待ちください。このメッセージが頻繁に出力され、通信できない場合は、メッセージ内容を弊社サービス拠点または弊社代理店まで連絡してください。
DSP busy	DSPのリソースが確保できない。	内部DSPリソースが空くまでお待ちください。このメッセージが頻繁に出力され、通信できない場合は、メッセージ内容を弊社サービス拠点または弊社代理店まで連絡してください。
no active port	使用可能なPRIポートが無いため発呼できない。	**「7.3.2　ケーブルの接続の確認」**を参照してください。

表B-8　CC:InFailの詳細メッセージの意味と対処

詳細メッセージ	意　味	対　処
lapd/layer1 error	下位層で障害が発生した。	頻繁に発生する場合には、ケーブルの接続を確認してください。
not enable	このPRIポートがenable状態になっていない。	このPRIポートの設定(boardsファイル)がenableになっていることを確認してください。
dstaddr/dstsubaddr not matched	このWANポートに設定されている自局電話番号(自局サブアドレス込み)と一致しない着呼を受けた。	このWANポートの自局電話番号の設定(boardsファイル)を確認してください。
clid refused	許可していない発信番号からの着呼を拒否した。	usersファイルに発信番号と一致するremote_telが登録されていることを確認してください。
clid require	boardsファイルのclid_ requireがonに設定されているため、発信者番号通知のない着呼を拒否した。	発信者番号通知のない着呼を拒否したい場合は、対処の必要はありません。
accept call off	usersファイルの%presetの項目accept_callがオフに設定されているため、着呼を拒否した。	着呼をすべて拒否したい場合は、対処の必要はありません。
incompatible	端末属性の一致しない着呼を拒否した。	発信元の端末の種類を確認してください。
STATUS received	STATUSメッセージを通知されたため、着呼処理を中止した。	対処の必要はありません。
RESTART received	RESTARTメッセージを通知されたため、着呼処理を中止した。	対処の必要はありません。

表B-9　L2MUX:InFailの詳細メッセージの意味と対処

詳細メッセージ	意　味	対　処
channel busy	内部チャネルリソースがビジーであるか、網指定チャネルがすでに使用中である。	内部チャネルリソースが空くまでお待ちください。
incompatible	端末属性の一致しない着呼を拒否した。	発信元の端末の種類を確認してください。

表B-10　CCMUX:InFailの詳細メッセージの意味と対処

詳細メッセージ	意　　味	対　　処
channel busy	Bチャネルのリソースが確保できない。	内部チャネルリソースが空くまでお待ちください。このメッセージが頻繁に出力され、通信できない場合は、メッセージ内容を弊社サービス拠点または弊社代理店まで連絡してください。
DSP busy	DSPのリソースが確保できない。	内部DSPリソースが空くまでお待ちください。このメッセージが頻繁に出力され、通信できない場合は、メッセージ内容を弊社サービス拠点または弊社代理店まで連絡してください。
imcompatible	端末属性の一致しない着呼を拒否した。	DSP拡張ボードが無い状態でモデムやPIAFSで着呼した可能性があります。

■ LCP Warningメッセージ

これは、PPPのLCPの接続／切断処理に関連するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:LCP(P1):P2:メッセージ

P1：識別情報

・NS-4200-10の場合

(Cw-x-y-z)

w ：PPP(LCP)が動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：ISDN回線の場合は発着信したPRIポートのBチャネル番号
高速ディジタル回線の場合はPRIポート内の論理チャネル番号で、boardsファイルの%channelで設定した論理チャネル番号

・NS-4200-30の場合

(Cx-y-z)

x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

上記以外に以下のように表示される場合があります。

(mm)

mm：本装置内部で管理している識別番号

P2：ユーザ名

相手局ユーザ名が表示されます。ただしユーザ名が特定できない場合は表示されません。

表B-11　Warningメッセージ一覧(LCP)

(1 / 2)

メッセージ	意　味	対　処
Connect Fail (Creq-Send-Retry-Out)	相手装置からCREQに対して応答がないため、LCPの確立に失敗した。(CREQの送信リトライアウト)	相手装置のPPPに関する設定および動作を確認してください。
Connect Fail (Treq-Recv)	LCP確立中に相手装置からTREQを受信したためLCPの確立に失敗した。	相手装置から切断されました。相手装置のPPPに関する設定および動作を確認してください。
Connect Fail (Cnak-Send-Retry-Out)	CNAKの送信リトライアウトが発生したため、LCPの確立に失敗した。	本装置PPPの設定と相手装置PPPの設定が一致していない可能性がありますので、使用するオプションを確認してください。主にPPP認証の設定が一致していない場合が考えられます。
Connect Fail (Crej-Send-Retry-Out)	CREJの送信リトライアウトが発生したため、LCPの確立に失敗した。	本装置PPPの設定と相手装置PPPの設定が一致していない可能性がありますので、使用するオプションの設定を確認してください。
Connect Fail (Cnak-Recv-Retry-Out)	CNAKの受信リトライアウトが発生したため、LCPの確立に失敗した。	本装置PPPの設定と相手装置PPPの設定が一致していない可能性がありますので、使用するオプションの設定を確認してください。
Connect Fail (Crej-Recv-Retry-Out)	CREJの受信リトライアウトが発生したため、LCPの確立に失敗した。	本装置PPPの設定と相手装置PPPの設定が一致していない可能性がありますので、使用するオプションの設定を確認してください。
Connect Fail (Auth-Nego-Fail)	本装置からの認証要求が拒否されたため、LCPの確立に失敗した。	本装置PPP認証の設定と相手装置の設定が一致していない可能性がありますので、使用するPPP認証の設定を確認してください。
Connect Fail (Callback-Nego-Fail)	本装置からのCBCP要求が拒否されたため、LCPの確立に失敗した。	本装置CBCPの設定と相手装置の設定が一致していない可能性がありますので、CBCPの設定を確認してください。
Connect Fail (Code-Reject)	相手装置からLCPのコードリジェクトを受信したためLCPの確立に失敗した。	相手装置のPPPに関する設定および動作を確認してください。
Connect Fail (IPCP-Protocol-Reject)	相手装置からIPCPのプロトコルリジェクトを受信したためLCPを切断した。	相手装置のPPPに関する設定および動作を確認してください。
Restart Retry-Out	LCPの再設定リトライアウトが発生したため、LCPを切断した。	特に対処する必要はありませんが、本メッセージが頻繁に出力される場合は、弊社サービス拠点または弊社代理店まで連絡してください。
Echo-Fail (Retry-Out)	相手装置からEcho(エコー)に対して応答がないため、LCPを切断した。	相手装置のPPPに関する設定および動作を確認してください。また、回線障害も考えられますので回線の状態を確認してください。

表B-11　Warningメッセージ一覧(LCP)

(2 / 2)

メッセージ	意　　味	対　　処
RESET (Options has changed)	LCPの再設定において、以前に確立したオプションと異なるオプションで再設定されたため、LCPを切断した。	相手装置のPPPに関する設定および動作を確認してください。
RESET (Auth Fail)	LCPの再設定でPPP認証に失敗したためLCPを切断した。	相手装置のPPPに関する設定および動作を確認してください。
Connect Fail(X)	(X)の理由により発信要求が失敗した。	本メッセージが頻繁に出力される場合は、(X)の理由表示を弊社サービス拠点または弊社代理店まで連絡してください。
Connect Fail (Call-Collition:X)	(X)のタイミングで発着信が衝突し、発信要求が失敗した。	時間をおいて再度発信してください。本メッセージが頻繁に出力される場合は、(X)のタイミング表示を弊社サービス拠点または弊社代理店まで連絡してください。
Connect Fail (Disconnected:Y)	LCPの処理中に切断された。詳細な処理(Y)については、下表を参照。	回線障害による下位レイヤの切断か、相手装置により切断された場合が考えられます。回線または相手装置側を確認してください。本メッセージが頻繁に出力される場合は、(Y)の処理表示を弊社サービス拠点または弊社代理店まで連絡してください。
Connect Refuse(X)	(X)の理由により着信を拒否した。	本メッセージが頻繁に出力される場合は、(X)の理由表示を弊社サービス拠点または弊社代理店まで連絡してください。

Y	内　容	フレームタイプ
1	発信によるLCPネゴシエーション中に下位レイヤが切断された。	HDLC
2	着信によるLCPネゴシエーション中に下位レイヤが切断された。	
3	ダイヤルアップユーザのPPP認証中に下位レイヤが切断された。	
4	MPでバンドル作成中に下位レイヤが切断された。	
m01	発信によるLCPネゴシエーション中に下位レイヤが切断された。	モデム（m） 1：V.32bis 2：V.34 3：K56flex 4：V.90 5：その他
m02	着信によるLCPネゴシエーション中に下位レイヤが切断された。	
m03	ダイヤルアップユーザのPPP認証中に下位レイヤが切断された。	
m04	MPでバンドル作成中に下位レイヤが切断された。	
p001	発信によるLCPネゴシエーション中に下位レイヤが切断された。	PIAFS（p） 1：V1.0 2：V2.0 3：V2.1 4：V2.2 5：その他
p002	着信によるLCPネゴシエーション中に下位レイヤが切断された。	
p003	ダイヤルアップユーザのPPP認証中に下位レイヤが切断された。	
p004	MPでバンドル作成中に下位レイヤが切断された。	

■ authd Warningメッセージ
これは、主にPPP認証(PAPあるいはCHAP)に関連するWarningメッセージです。
次のようなフォーマットになっています。<X>の部分がない場合もあります。

[CID ****]:authd:メッセージ<X>

X：相手局のユーザ名

表B-12　Warningメッセージ一覧(authd)

(1 / 2)

メッセージ	意　　味	対　　処
PAP refuse (Unknown Name<X>)	相手局が通知してきたユーザ名が不正のため拒否した。	相手局のユーザ名がusersファイルに登録されているか確認してください。RADIUS認証を使用する場合には、radiusファイルのmodeがonになっているか確認してください。
PAP refuse (Unknown Name)	相手局が通知してきたユーザ名の長さが不正のため拒否した。	相手装置のPPPの設定等を確認してください。
PAP refuse (Unknown Password<X>)	相手局が通知してきたパスワードが不正のため拒否した。	usersファイルに登録されている相手局のパスワードを確認してください。
PAP refuse (Radius Unknown User<X>)	RADIUS認証サーバが拒否した。	RADIUS認証サーバに登録されている、相手局のユーザ名/パスワードなどの情報が正しく登録されているか確認してください。
PAP refuse (Wait Timeout)	相手局のPAPが無応答。(PAP要求が到達しない)	相手装置のPPPの設定等を確認してください。
PAP refuse (Radius No Reply<X>)	RADIUS認証サーバからの応答がない。	RADIUS認証サーバの設定および本装置のradiusファイルの設定を確認してください。
PAP fail (Remote Refuse)	ユーザ名あるいはパスワードが不正のため相手局が拒否した。	usersファイルに登録されている自局のユーザ名/パスワードを確認してください。
PAP fail (No Reply)	相手局PAPが無応答。(PAP要求に対する応答がない)	相手装置のPPPの設定等を確認してください。
CHAP refuse (Unknown Name<X>)	相手局が通知してきたユーザ名が不正のため拒否した。	相手局のユーザ名がusersファイルに登録されているか確認してください。RADIUS認証を使用する場合には、radiusファイルのmodeがonになっているか確認してください。
CHAP refuse (Unknown Name)	相手局が通知してきたユーザ名の長さが不正のため拒否した。	相手装置のPPPの設定等を確認してください。
CHAP refuse (Invalid Response<X>)	相手局が通知してきたレスポンス値が不正のため拒否した。	相手局に対するパスワードと相手のパスワードが一致しているか確認してください。

表B-12　Warningメッセージ一覧(authd)

(2 / 2)

メッセージ	意　味	対　処
CHAP refuse (Radius Unknown User<X>)	RADIUS認証サーバが拒否した。	RADIUS認証サーバに登録されている相手局のユーザ名/パスワードなどの情報が正しく登録されているか確認してください。
CHAP refuse (No Reply(Response))	相手局のCHAPが無応答。(レスポンスなし)	相手装置のPPPの設定等を確認してください。
CHAP refuse (Radius No Reply<X>)	RADIUS認証サーバからの応答がない。	RADIUS認証サーバの設定および本装置のradiusファイルの設定を確認してください。
RX:CHAP-Code-Error(X)	CHAP認証中に不正なコード(X)のパケットを受信した。	本メッセージは、Windows95で接続時、CHAP-Responseの再送が発生すると不正なコード（0x5）のパケットを受信することが確認されています。この場合は、特に対処する必要はありません。ただし、本メッセージが頻繁に出力され、接続できない場合は、別の原因が考えられます。本装置のradiusファイルの設定やRADIUS認証サーバの設定を確認してください。
CHAP fail (Remote Refuse)	ユーザ名/レスポンス値が不正のため相手が拒否した。	自局のユーザ名が相手に登録されているか、相手局に対するパスワードが相手のパスワードと一致しているかを確認してください。
CHAP fail (No Reply)	相手局のCHAPが無応答（結果のレスポンスなし)。	相手装置のPPPの設定等を確認してください。
CHAP fail (Wait Timeout)	相手局のCHAPが無応答（Challenge が到達しない)。	相手装置のPPPの設定等を確認してください。
CHAP fail (No Password<X>)	パスワードが設定されていない。	usersファイルに登録されている相手局に対するパスワードを確認してください。
authType error([y:z] is not supported)	本装置ではサポートしていない認証方式の組み合わせ(y：相手に要求する認証方式、z：相手から要求される認証方式)であるため、拒否した。	本装置および相手装置の認証方式の設定を確認してください。
refuse (PPPauth-suucess, CLIDauth-fail<X>)	PPP認証は成功したが、CLID認証が失敗したので拒否した。	usersファイルのユーザxに対するCLID認証の設定、電話番号の設定を確認してください。
refuse (Accept-call inhibit<X>)	このユーザ（X）に対して「accept_call off」の設定がされている。	usersファイルの設定を確認してください。 このユーザに対して着信を許可していないのであれば、特に対処する必要はありません。

■ MPs Warningメッセージ

これは、主にPPPあるいはMPの接続処理に関連するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:MPs:メッセージ(X)

X：相手局のユーザ名
（ユーザ名がない場合、"-"が入ります）

表B-13　Warningメッセージ一覧(MPs)

(1 / 2)

メッセージ	意　味	対　処
no channel resource	enableになっているポートまたは、指定したポートが全て使用されているため、発呼できない。	チャネルが空くまで待つか、usersファイルのportの設定を確認してください。
exceeded mp_port_max	MP使用時に、最大リンク数を越えてリンクを追加しようとした。	usersファイルのmp_port_maxの設定を確認してください。
remote telephone number is empty	相手電話番号がないのに発呼しようとした。	usersファイルにremote_telを設定しているか確認してください。
remote telephone number for calling is not found	MP使用時に、リンク追加時に相手電話番号が見つからなかった。	usersファイルにremote_telを設定しているか確認してください。
connect refuse:user name already in use	すでに使用中のユーザと同じユーザが着呼したため、拒否した。	特に対処は必要ありません。
connect refuse:port preempted	コールバック（発呼）しようとしたチャネルに着呼したため、その着呼を拒否した。（コールバック優先）	特に対処は必要ありません。
connect fail:call collision	同じチャネルで発呼中に着呼を受け付けたので、発呼が失敗した。	特に対処は必要ありません。
user collision	同じユーザの発呼と着呼が衝突し、片側を切断した。	特に対処は必要ありません。
logical interface is disable	ポートがdisableになっている。	ポートの設定(boardsファイルのenable／disable)を確認してください。

表B-13　Warningメッセージ一覧(MPs)

(2 / 2)

メッセージ	意　　味	対　　処
different PPP information(y)	MP使用時に、リンク追加しようとしたが、PPPの情報が異なっていたので、切断した。 y＝異なっていた情報 110：ユーザ名 111：プロトコル 112：EID	PPPのユーザ名、パスワード、プロトコルおよび、接続相手先のPPPの設定値などを確認してください。
port mismatch	着呼したポートが指定したポートと異なっていたので、切断した。	usersファイルのportの設定を確認してください。

■ BACP Warningメッセージ

これは、主にBACPの接続／切断処理に関連するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:BACP:ユーザ名:メッセージ

表B-14　Warningメッセージ一覧(BACP)

メッセージ	意　　味	対　　処
Connect Fail (Cnak-Send-Retry-Out)	BACPの必須オプション (Favored-Peer) のネゴシエーションが正しく行われなかったので、BACPのコネクション確立に失敗した。 (Configuration-NAK送信リトライアウト)	相手側装置の設定等を確認してください。
Connect Fail (Crej-Sen-Retry-Out)	相手側BACPが無効なオプションを要求しているので、BACPのコネクション確立に失敗した (Configuration-Reject送信リトライアウト)	相手側装置の設定等を確認してください。
Connect Fail (Cnak-Recv-Retry-Out)	BACPの必須オプション (Favored-Peer) のネゴシエーションが正しく行われなかったので、BACPのコネクション確立に失敗した。 (Configuration-NAK受信リトライアウト)	相手側装置の設定等を確認してください。
Connect Fail (Crej-Recv-Retry-Out)	BACPの必須オプション (Favored-Peer) のネゴシエーションが正しく行われなかったので、BACPのコネクション確立に失敗した。 (Configuration-Reject受信リトライアウト)	相手側装置の設定等を確認してください。

■ **BAP Warningメッセージ**

これは、主にBAPのリンク追加／リンク削除処理に関連するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:BAP:ユーザ名:メッセージ

表B-15　Warningメッセージ一覧(BAP)

メッセージ	意　味	対　処
OutFail (ReqSent:CallReq-Send-Retryout)	相手側BAPが応答しないので、リンク追加要求に失敗した。(CallRequest送信リトライアウト)	相手側装置の設定等を確認してください。
OutFail (ReqSent:CallReq-Rejected)	相手側BAPがリンク追加要求を拒否したため、リンク追加要求に失敗した。	相手側装置の設定等を確認してください。
OutFail (ReqSent:No-Remote-Telnumber)	相手側BAPが電話番号を通知してこなかったため、リンク追加要求に失敗した。	相手側装置の設定等を確認してください。または、ローカル認証(PPP認証／CLID認証)の場合は、本装置に相手側装置の電話番号(remote_tel)を設定してください。
InFail (No-Callback-Accept)	相手装置からのコールバックリンク追加要求を受け入れなかった。	相手側装置からBAPのコールバックリンク追加要求を発行しないように設定してください。
InFail (Link-Add-Wait-Timeout)	相手装置からリンク追加要求を受け入れたが、ある一定時間(30s)たっても相手装置からリンクが追加されなかった。または、リンクの追加は正常に行われたが、その結果通知(StatusInd)が行われなかった。	相手側装置の設定等を確認してください。

■ ncpd/NCP Warningメッセージ

これは、PPPのNCP(IPCP)関連のメッセージです。
次のようなフォーマットになっています。

[CID ****]:ncpd(X):ユーザ名:メッセージ
[CID ****]:NCP(X):ユーザ名:メッセージ

X：本装置内部で管理しているNCPの識別番号

表B-16　Warningメッセージ一覧(ncpd/NCP)

(1 / 2)

メッセージ	意　味	対　処
no ippool address (pool No.[n])	IPアドレスをプール番号n番のプールから取得できなかった。	ippoolファイルの設定を確認してください。
IPCP:Connect Fail (Creq-Send-Retry-Out)	IPCPコネクション確立に失敗した。(Configuration-Request送信リトライアウト)	相手PPPが応答していません。相手側装置の設定を確認してください。
IPCP:Connect Fail (Cnak-Send-Retry-Out)	IPCPコネクション確立に失敗した。(Configuration-NAK送信リトライアウト)	自局PPPの設定と相手側装置の設定が一致していません。IPCPで使用するオプションを確認してください。
IPCP:Connect Fail (Crej-Send-Retry-Out)	IPCPコネクション確立に失敗した。(Configuration-Reject送信リトライアウト)	自局PPPの設定と相手側装置の設定が一致していません。IPCPで使用するオプションを確認してください。
IPCP:Connect Fail (Cnak-Recv-Retry-Out)	IPCPコネクション確立に失敗した。(Configuration-NAK受信リトライアウト)	自局PPPの設定と相手側装置の設定が一致していません。IPCPで使用するオプションを確認してください。
IPCP:Connect Fail (Crej-Recv-Retry-Out)	IPCPコネクション確立に失敗した。(Configuration-Reject受信リトライアウト)	自局PPPの設定と相手側装置の設定が一致していません。IPCPで使用するオプションを確認してください。
IPCP:Restart Retry-Out	IPCPコネクションの再設定が規定回数以上行われたため、IPCPコネクションを切断した。	特に対処する必要はありません。 本メッセージが頻繁に出力される場合は、弊社サービス拠点または弊社代理店までご連絡ください。
IPCP:Connect Fail (disconnected)	IPCP確立前に、下位レイヤ(LCP/ISDN)が切断された。	相手側装置の設定を確認してください。

表B-16　Warningメッセージ一覧(ncpd/NCP)

(2 / 2)

メッセージ	意　味	対　処
reload now in progress	reloadコマンドを実行中に接続された。	reloadコマンドが完了してから、再度接続してください。
user's information changed	接続中にreloadコマンドでユーザ情報が変わってしまった。	再度接続してください。
route already in use	ルーティング情報がすでに使われている。	usersファイルのdestinationの指定を他のユーザと重複しないようにしてください。 同じユーザの発信と着信が同時に発生した場合にも、このメッセージが出力されますが、このときには対処の必要はありません。
invalid gateway	ゲートウェイの指定が不正である。	usersファイルのdestinationの部分で、ゲートウェイの指定を正しくしてください。interfaceの部分で指定した相手アドレスと同じにしてください。
duplicate proxy address (x.x.x.x)	プロキシARPで設定するIPアドレス(x.x.x.x)が重複している。	usersファイルで相手に割り当てるIPアドレスを重複しないように指定してください。

■ isdncb Warningメッセージ

これは、無課金コールバックに関するWarningメッセージです。
次のようなフォーマットになっています。

isdncb:ユーザ名:メッセージ

表B-17　Warningメッセージ一覧(isdncb)

メッセージ	意　味	対　処
Callback Fail (user's information changed)	着信があってから、コールバックするまでの間に、ユーザ情報が変更されたため、コールバック処理を中止した。	本装置がコールバックする直前に、reloadコマンドを実行した場合、このエラーになることがあります。再度接続してください。
Callback Fail (no user's information)	着信があってから、コールバックするまでの間に、ユーザ情報が削除されたため、コールバック処理を中止した。	本装置がコールバックする直前に、reloadコマンドを実行した場合、このエラーになることがあります。再度接続してください。
Callback Fail (now in progress)	着信があってから、コールバックするまでの間に、同じユーザから再び着信した。新しい着信に対するコールバックは行わない。	相手装置のコールバック関連の設定を確認してください。
Callback Fail (resource busy)	リソースの関係で、コールバックに失敗した。	少し待ってから、再度接続してください。

■ CBCP Warningメッセージ

これは、CBCPのコールバックに関するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:CBCP(P1):P2:メッセージ

P1：識別情報

・NS-4200-10の場合
(Cw-x-y-z)
w ：CBCPが動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

・NS-4200-30の場合
(Cx-y-z)
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

P2：ユーザ名

相手局ユーザ名が表示されます。ただしユーザ名が特定できない場合は表示されません。

表B-18 Warningメッセージ一覧(CBCP)

(1 / 2)

メッセージ	意　味	対　処
Connect Refuse (Callback-busy)	コールバック処理中に同一ユーザから続けて着呼したため、その着呼は拒否した。	特に対処する必要はありません。時間をおいて再度発呼してください。
Connect Refuse (Callback-only)	コールバック要求のみ受け入れる設定 (cb_mode must)になっているため、通常の着呼を拒否した。	相手装置のコールバック関連の設定を確認してください。
OutFail (No-Caller/Answerer-Option)	CBCPのコールバック要求時、相手から有効なオプションが通知されなかったため、コールバックに失敗した。	相手装置のコールバック関連の設定を確認してください。
OutFail (No-Local-TelNumber)	CBCPのコールバック要求時、自局電話番号が求められなかった。	自局電話番号(boardsファイル)が設定されているか確認してください。

表B-18　Warningメッセージ一覧(CBCP)

(2 / 2)

メッセージ	意　味	対　処
OutFail (CBCPreq-Wait-Timeout)	CBCPのコールバック要求時、相手からCBCPのパケットが通知されなかったため、コールバックに失敗した。(CallbackRequest受信タイムアウト)	相手装置のコールバック関連の設定を確認してください。
OutFail (CBCPrsp-Send-Retryout)	CBCPのコールバック要求時、相手から応答が無いためコールバックに失敗した。(CallbackResponse送信リトライアウト)	相手装置のコールバック関連の設定を確認してください。
OutFail (Disconnected)	CBCPのコールバック要求発行後、CBCPのネゴシエーション実行中に切断された。	回線障害による下位レイヤの切断か、相手装置により切断された場合が考えられます。 回線または相手装置を確認してください。
InFail (CBCPreq-Send-Retryout)	CBCPのコールバック要求受け入れ時、相手から応答が無いためコールバックに失敗した。(CallbackRequest送信リトライアウト)	相手装置のコールバック関連の設定を確認してください。
InFail (CBCPrsp-Invalid-Option)	CBCPのコールバック要求受け入れ時、相手から無効なオプションが通知されたためコールバックに失敗した。	相手装置のコールバック関連の設定を確認してください。
InFail (Callback-Protocol-Mismatch)	受け入れたコールバック方式と本装置の設定が一致しないため接続に失敗した。	本装置のコールバック方式の設定(cb_type)と相手装置のコールバック関連の設定を確認してください。
InFail (Disconnected)	CBCPのコールバック要求受け入れ後、CBCPのネゴシエーション実行中に切断された。	回線障害による下位レイヤの切断か、相手装置により切断された場合が考えられます。 回線または相手装置を確認してください。

■ radiusd/acctd Warning メッセージ

これは、RADIUSサーバとの通信に関連するWarningメッセージです。

表B-19　Warningメッセージ一覧(radiusd/acctd)

(1 / 2)

メッセージ	意　味	対　処
radiusd:No host	RADIUSサーバーのhostが設定されていない。	radiusファイルにRADIUSサーバのhost (host1, host2, host3)を設定してください。
radiusd:Radius retry timeout	RADIUS サーバからの応答がないか、不正な応答であったため、Requestを再送したが、設定再送回数に達したため送信をやめた。	(1) RADIUSサーバが起動されているか確認してください。 (2) radiusファイルのport番号が登録されているものと一致しているか確認してください(デフォルトは1645)。 (3) radiusファイルのtimeout(再送間隔)とretry (再送回数)を変更して応答が受信できるように調節してください。 (4) “ Strange radius reply ”Warninngメッセージが出力されている場合、それに従った対処をしてください。
radiusd:Strange radius reply.Invalid Authenticator	RADIUSサーバから不正な応答を受信したため、無視した。	radiusファイルのkeyが RADIUSサーバに登録されているものと同じであるか確認してください。

表B-19　Warningメッセージ一覧(radiusd/acctd)

(2 / 2)

メッセージ	意　味	対　処
acctd:No host	RADIUS アカウントサーバーのhostが設定されていない。	radiusファイルにRADIUSアカウントサーバのhost(host1, host2, host3)を設定してください。
acctd:Radius retry timeout	RADIUSアカウントサーバからの応答がないか、不正な応答であったため、Requestを再送したが、設定再送回数に達したため送信をやめた。	(1) RADIUSアカウントサーバが起動されているか確認してください。 (2) radiusファイルのport番号が登録されているものと一致しているか確認してください(デフォルトは1646)。 (3) radiusファイルのtimeout(再送間隔)とretry (再送回数)を変更して応答が受信できるように調節してください。 (4) “ Strange radius reply ” Warninng メッセージが出力されている場合、それに従った対処をしてください。
acctd:Strange radius reply.Invalid Authenticator	RADIUSアカウントサーバから不正な応答を受信したため、無視した。	radiusファイルのkeyが RADIUSアカウントサーバに登録されているものと同じであるか確認してください。

■ acctdアカウント情報

このメッセージは、RADIUSアカウントサーバに何らかの理由でアカウントを送信できなかった場合に consoleに出力されます。
次のようなフォーマットになっています。

acctd:[(ST)start(UN)ns2482(SI)d9000018]
acctd:[(ST)stop(UN)ns2482(SI)d9000018(TM)0(IO)43(OO)9]

(ST)：　Acct-Status-Type

(UN)：　ユーザ名

(SI)：　Acct-Session-Id

(TM)：　Acct-Session-Time

(IO)：　Acct-Input-Octets

(OO)：　Acct-Output-Octets

■ RADIUSserver Warningメッセージ

これは、RADIUS認証サーバから受信した認証結果の解析において出力されるWarningメッセージです。
次のようなフォーマットになっています。

RADIUSserver:メッセージ

表B-20　Warningメッセージ一覧(RADIUSserver)

メッセージ	意　味	対　処
invalid Filter-Id(X)	受信したFilter-Idのフィルタ名(X)が正しくない。	RADIUS認証サーバのFilter-Idの設定を確認してください。
already specified filter Filter-Id,ignored	すでに指定されているFilter-Idを受信した。	RADIUS認証サーバで同じユーザに対して同じFilter-Idを設定している可能性がありますので確認してください。
already specified include Filter-Id,ignored	すでに指定されているaccess-includeのFilter-Idを受信した。	RADIUS認証サーバで同じユーザに対して同じaccess-includeのFilter-Idを設定している可能性がありますので確認してください。
already specified exclude Filter-Id,ignored	すでに指定されているaccess-excludeのFilter-Idを受信した。	RADIUS認証サーバで同じユーザに対して同じaccess-excludeのFilter-Idを設定している可能性がありますので確認してください。
undefined filter Filter-Id(X),ignored	ipfiltersファイルに登録されていないFilter-Id(X)を受信した。	RADIUS認証サーバのFilter-Idの設定、および本装置のipfiltersファイルに登録されているフィルタ名を確認してください。
invalid Framed-Route,ignored	書式の正しくないFramed-Routeを受信した。	RADIUS認証サーバのFramed-Routeの書式が正しく設定されているか確認してください。
undefined filter Framed-Route(X),ignored	ipfiltersファイルに登録されていないフィルタ名(X)を指定したFramed-Routeを受信した。	RADIUS認証サーバのFramed-Routeの設定、および本装置のipfiltersファイルに登録されているフィルタ名を確認してください。
Session-Time(X) out of range,selected max value (100000)	受信したSession-Timeoutの値(X)が本装置のMAX値を超えていたので、本放置のMAXに設定された。	RADIUS認証サーバのSession-Timeoutの設定値を本装置の設定範囲内（5～100000）に設定してください。
Idle-Time(X) out of range,selected max value (100000)	受信したIdle-Timeoutの値(X)が本装置のMAX値を超えていたので、本放置のMAXに設定された。	RADIUS認証サーバのIdle-Timeoutの設定値を本装置の設定範囲内（5～100000）に設定してください。
invalid ippool(X)	受信したAssign-IP-Poolの番号(X)が、本装置のIPpoolの範囲を超えていた。	RADIUS認証サーバのAssign-IP-Poolの設定値を本装置の設定範囲内（0～16）に設定してください。

■ **snmpd Warningメッセージ**

これは、SNMPの動作に関するWarningメッセージです。
次のようなフォーマットになっています。

snmpd:メッセージ

表B-21　Warningメッセージ一覧(snmpd)

メッセージ	意　味	対　処
authentication failure (from x.x.x.x)	snmpconfファイルに登録されていないコミュニティでSNMPマネージャからアクセスされた。(x.x.x.xはSNMPマネージャのIPアドレス)	snmpconfファイルのcommunity の設定を確認してください。SNMPマネージャの設定を確認してください。
unexpected manager IP address x.x.x.x	snmpconfファイルに登録されていないIPアドレスのSNMPマネージャからアクセスされた。(x.x.x.xはSNMPマネージャのIPアドレス)	snmpconfファイルのcommunity の設定を確認してください。SNMPマネージャの設定を確認してください。
request message format error (from x.x.x.x)	受信したSNMPパケットのフォーマットに誤りがある。(x.x.x.xはSNMPマネージャのIPアドレス)	SNMPマネージャの仕様を確認してください。

■ routed Warningメッセージ

これは、RIPの動作に関するWarningメッセージです。
次のようなフォーマットになっています。

routed: メッセージ

表B-22　Warningメッセージ一覧(routed)

メッセージ	意　　味	対　　処
port number miss match	ポート番号が一致しない。	送信元の装置のRIPの設定を確認してください。
packet from unknown router or host, x.x.x.x	未知のルータまたはホストx.x.x.xからパケットを受信した。 (x.x.x.xはIPアドレス)	rip.confファイルに論理インタフェースが設定されているか確認してください。
authentication fail, from x.x.x.x	x.x.x.xからのパケットが認証に失敗した。 (x.x.x.xはIPアドレス)	rip.confファイルの認証の設定または送信元の認証の設定を確認してください。
interface coming up, XXX	論理インタフェースXXXがアップした。 (XXXは論理インタフェース名)	特に対処する必要はありません。
interface going down, XXX	論理インタフェースXXXがダウンした。 (XXXは論理インタフェース名)	ケーブルが接続されているか確認してください。

■ **DSPC Warningメッセージ**

これは、本装置のDSPを使用して行われるモデム通信およびPIAFS通信に関連するWarningメッセージです。
次のようなフォーマットになっています。

[CID ****]:DSPC(P1):P2:メッセージ

P1：識別情報1

(m-n)
m　：DSPを収容しているDSPボードのスロット番号
n　：DSP番号

P2：識別情報2

・NS-4200-10の場合
(Cw-x-y-z)
w　：DSPCが動作しているDSPボードのスロット番号
x　：発着信したPRIボードのスロット番号
y　：発着信したPRIボードのポート番号
z　：発着信したPRIポートのBチャネル番号

・NS-4200-30の場合
(Cx-y-z)
x　：発着信したPRIボードのスロット番号
y　：発着信したPRIボードのポート番号
z　：発着信したPRIポートのBチャネル番号

表B-23　Warningメッセージ一覧(DSPC)

メッセージ	意　味	対　処
STOP (MODEM:C1:C2)	モデム接続が失敗した。 C1,C2：内部コード	何回も連続して接続に失敗する場合、**7.3.4**項**(2)**を参照してください。
STOP (PIAFSxx:C1:C2)	PIAFS接続が失敗した。 xx：PIAFSのバージョン 10：V1.0 20：V2.0 21：V2.1 C1,C2：内部コード	通信相手の電波状況が良くない場合があります。 場所、時間帯を変えて接続してみてください。

■ boards Warningメッセージ

これは、起動時あるいはreloadコマンド実行時にboardsファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

boards(line N):メッセージ

N：セットアップファイルの行番号

表B-24　Warningメッセージ一覧(boards)

(1 / 3)

メッセージ	意　味	対　処
argument too less[X] (the line ignored).	キーワードの引数[X]が少ない。 この行は無視された。	N行目の引数を正しく設定してください。
can't use '%channel' with line_type isdn(the entry ignored).	ISDN回線で%channelキーワードを使用した。 このエントリは無視された。	line_type isdnで%channelキーワードを使用する必要はありません。
duplicate channel number[X] (the line ignored).	拡張ボード内で論理チャネル番号[X]が重複した。 この行は無視された。	N行目の論理チャネル番号を変更してください。
duplicate port number[X] (the line ignored).	拡張ボード内でポート番号[X]が重複した。 この行は無視された。	N行目のポート番号を変更してください。
duplicate timeslot[X] (the line ignored).	タイムスロット[X]が他のチャネルと重複した。 この行は無視された。	タイムスロットが重ならないように設定してください。
illegal argument[X] (the line ignored).	キーワードに正しくない引数[X]が指定された。 この行は無視された。	N行目の引数を確認してください。
inconsistent channel with service (the entry ignored).	回線種別と論理チャネルの設定が矛盾している。 このエントリは無視された。	N行目の回線種別と論理チャネルの設定を確認してください。
invalid '%board' number (the line ignored).	%boardで指定したボード番号が範囲外である。 この行は無視された。	N行目の拡張ボードスロット番号を確認してください。
invalid argument[X] (the line ignored).	キーワードの引数[X]が範囲外である。 この行は無視された。	N行目の引数を確認してください。
invalid channel speed (the entry ignored).	チャネル速度が範囲外である。 このエントリは無視された。	N行目のエントリのタイムスロットを確認してください。
invalid time slots(the entry ignored).	タイムスロットが範囲外である。 このエントリは無視された。	N行目のエントリのタイムスロットを確認してください。

表B-24　Warningメッセージ一覧(boards)

(2 / 3)

メッセージ	意　味	対　処
keyword '%board' required (the line ignored).	この行はキーワード%boardが必要である。 この行は無視された。	この行の前にキーワード%boardを設定してください。
keyword '%channel' or '%port' required[X] (the line ignored).	この行のキーワード[X]は%channelか%portが必要である。 この行は無視された。	N行目の前にキーワード%channelか%portを設定してください。
keyword '%channel' required [X] (the line ignored).	この行のキーワード[X]は%channelが必要である。 この行は無視された。	N行目の前にキーワード%channelを設定してください。
keyword '%port' require[X] (the line ignored).	この行のキーワード[X]は%portが必要である。 この行は無視された。	N行目の前にキーワード%portを設定してください。
line type required (the entry ignored).	この行は回線種別が必要である。 このエントリは無視された。	N行目の前にキーワードline_typeを設定してください。
mismatch line type[X] (the line ignored).	未対応の回線種別[X]が指定された。 この行は無視された。	回線種別を変更してください。
no channel (the entry ignored).	ポートに論理チャネルが設定されていない。 このエントリは無視された。	論理チャネルを設定してください。
no ext-board in slot[X] (the line ignored).	指定されたスロット番号[X]に拡張ボードがない。 この行は無視された。	拡張ボードがある拡張ボードスロット番号を指定してください。
not support speed (the entry ignored).	未サポートの速度が指定された。 このエントリは無視された。	タイムスロットの設定を確認してください。
please reboot for modified 'line_type'.	回線種別が変更されたので再起動が必要である。	設定を保存後、再起動してください。
please reboot for modified channel.	論理チャネルの設定が変更されたので再起動が必要である。	設定を保存後、再起動してください。
please reboot for modified port.	ポートの設定が変更されたので再起動が必要である。	設定を保存後、再起動してください。

表B-24　Warningメッセージ一覧(boards)

(3 / 3)

メッセージ	意　　味	対　　処
syntax error[X] (the line ignored).	キーワード[X]の構文エラー。 この行は無視された。	N行目を確認してください。
too many options[X] (the line ignored).	キーワードのオプション[X]が多過ぎる。 この行は無視された。	N行目のオプションを確認してください。
unknown keyword[X] (the line ignored).	未定義のキーワード[X]が検出された。 この行は無視された。	N行目のキーワードを確認してください。
unknown line type (the entry ignored).	回線種別が未定義である。 このエントリは無視された。	N行目のline_typeを確認してください。
unknown line type[X] (the line ignored).	回線種別[X]が未定義である。 この行は無視された。	N行目のline_typeを確認してください。

■ users Warningメッセージ

これは、起動時あるいはreloadコマンド実行時にusersファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

users(line N):メッセージ

N：セットアップファイルの行番号
（行番号がない場合もあります）

表B-25　Warningメッセージ一覧(users)

(1 / 3)

メッセージ	意　味	対　処
invalid keyword(Y)	設定されているキーワード(Y)が正しくない。	N行目のキーワードの設定を確認してください。
invalid symbol(%Y) (ignored to line Z)	設定されている分類キーワード(%Y)が正しくないので、Z行目までの設定が無視された。	N行目の分類キーワードの設定を確認してください。
[Y] can't use in current symbol	直前にある分類キーワードでは使用できないキーワード[Y]が指定された。	N行目のキーワードの設定を確認してください。
parameter isn't specified	キーワードに対するパラメータが設定されていない。	N行目のキーワードの設定を確認してください。
invalid parameter(Y)	キーワードに対するパラメータ(Y)の設定が正しくない。	N行目のパラメータの設定を確認してください。
too long name(Y)	ユーザ名(Y)の長さが本装置のMAX(64)を超えている。	N行目のユーザ名の設定(local_nameあるいはremote_name)を確認してください。
too long passwd(Y)	パスワード(Y)の長さが本装置のMAX(32)を超えている。	N行目のパスワードの設定(local_passwdあるいはremote_passwd)を確認してください。
invalid telnumber(Y)	電話番号(Y)の書式が正しくない。	N行目の電話番号の設定を確認してください。
invalid time value(Y) (range is 5~60000)	タイムアウト時間の設定値(Y)が正しくない。	N行目のタイムアウト時間を範囲に収まる値に設定してください。
unknown host or invalid IP address (Y)	設定されているIPアドレス(Y)が正しくない。	N行目のIPアドレスの設定を確認してください。
symbol not found	分類キーワードが設定される前に、キーワードが指定された。	キーワードは分類キーワードの設定の後ろに設定する必要があります。N行目の設定を確認してください。
symbol[Y] already specified (ignored to line Z)	Y(%presetあるいは%default)が複数設定されているため、Z行目まで設定が無視された。	2つ目以降の%presetあるいは%defaultの設定は無効になりますので、N行目からの設定を確認してください。

表B-25　Warningメッセージ一覧(users)

(2 / 3)

メッセージ	意　味	対　処
This %user isn't specified remote_name & remote_tel.	この%userのエントリには、remote_nameもremote_telも設定されていない。	着信を受け付けるためには、CLID認証あるいはPPP認証を行う必要がありますので、設定を確認してください。
too many tels are specified(max=Y).	電話番号が本装置のMAX(Y)以上設定されている。	その%userで設定する電話番号(remote_telあるいはaccept_tel)をMAX以下にしてください。
undefined filter, ignore this line.	定義されていないフィルタである。 この行は無視された。	指定したフィルタがipfiltersファイルで定義されているか確認してください。
unknown ppp option, ignore this line.	未定義のpppオプションである。 この行は無視された。	pppサブキーワードの設定を確認してください。
filter already specified, ignore this line.	フィルタはすでに指定してある。 この行は無視された。	filterサブキーワードを複数指定していないか確認してください。
unknown flag, ignore this line.	未定義のフラグである。 この行は無視された。	unnumbered、numbered、downなどの設定が正しいか確認してください。
unknown argument, ignore this line.	未定義のアーギュメントである。 この行は無視された。	N行目のアーギュメントを確認してください。
filter name required, ignore this line.	フィルタ名が必要である。 この行は無視された。	フィルタ名を追加してください。
'include' or 'exclude' required, ignore this line.	'include'または'exclude'が必要である。 この行は無視された。	アクセスフィルタの設定を確認してください。
number required, ignore this line.	番号が必要である。 この行は無視された。	番号で指定してください。
invalid argument, ignore this interface.	正しくないアーギュメントである。 このインタフェースは無視された。	N行目のアーギュメントを確認してください。
hostname invalid or unknown, ignore this interface.	ホスト名が正しくないか未定義である。 このインタフェースは無視された。	ホスト名を確認してください。また、hostsファイルに登録されているか確認してください。
invalid prefix specification, ignore this interface.	正しくないprefix設定である。 このインタフェースは無視された。	N行目のマスクの設定を確認してください。
interface-specifier invalid, ignore this interface.	論理インタフェース名が正しくない。 このインタフェースは無視された。	N行目の論理インタフェース名を確認してください。
invalid destination, ignore this interface.	正しくないデスティネーションである。 このインタフェースは無視された。	N行目のデスティネーションの設定を確認してください。

表B-25　Warningメッセージ一覧(users)

(3 / 3)

メッセージ	意　味	対　処
number required, ignore this interface.	番号が必要である。このインタフェースは無視された。	番号で指定してください。
interface name required, ignore this interface.	論理インタフェース名が必要である。このインタフェースは無視された。	論理インタフェース名を指定してください。
invalid flag, ignore this interface.	正しくないフラグである。このインタフェースは無視された。	unnumbered、numbered、downなどの設定が正しいか確認してください。
prefix specification range error, ignore this interface.	prefix設定のとりうる範囲外である。このインタフェースは無視された。	マスクの設定を確認してください。
invalid cost, ignore this interface.	正しくない送信コストである。このインタフェースは無視された。	コストの設定を確認してください。
gateway syntax error, ignore this interface.	ゲートウェイの構文エラーである。このインタフェースは無視された。	N行目のゲートウェイの設定を確認してください。
syntax error, ignore this interface.	構文エラー。このインタフェースは無視された。	N行目の設定を確認してください。
couldn't find default local address.	default local addressを見つけられなかった。	hostnameファイルおよびhostsファイルの設定を確認してください。
invalid option, ignore this route.	正しくないオプションである。このルートは無視された。	N行目の設定を確認してください。
destination address required, ignore this route.	宛先アドレスが必要である。このルートは無視された。	宛先アドレスを指定してください。
'via' required, ignore this route.	キーワード'via'が必要である。このルートは無視された。	キーワード'via'を指定してください。
gateway required, ignore this route.	ゲートウェイが必要である。このルートは無視された。	ゲートウェイを指定してください。
cost range error (1~99), ignore this route.	送信コストが1～99の範囲外である。	コストの設定を確認してください。
gateway syntax error, ignore this route.	ゲートウェイの構文エラー。このルートは無視された。	N行目の設定を確認してください。
invalid format (slot/port)	portキーワードの書式エラーである。	“拡張ボードスロット番号／ポート番号”のように指定してください。
invalid slot number(Y) (range is 1~4)	拡張ボードスロット番号(Y)は範囲外である。	拡張ボードスロット番号には1から4の値を指定してください。
invalid port number(Y) (range is 1~6)	ポート番号(Y) は範囲外である。	ポート番号には1から6の値を指定してください。

■ radius Warningメッセージ

これは、起動時あるいはreloadコマンド実行時にradiusファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

radius(line N):メッセージ

N：セットアップファイルの行番号

表B-26　Warningメッセージ一覧(radius)

メッセージ	意　味	対　処
invalid keyword(Y)	設定されているキーワード(Y)が正しくない。	N行目のキーワードの設定を確認してください。
invalid symbol(Y)	設定されている分類キーワード(Y)が正しくない。	N行目の分類キーワードの設定を確認してください。
unknown host or invalid IP address	設定されているIPアドレスが正しくない。	N行目のIPアドレスの設定を確認してください。
too long passwd(Y)	key(Y)の長さが本装置のMAX(16)を超えている。	N行目のkeyの設定を確認してください。
invalid parameter(Y)	キーワードに対するパラメータ(Y)の設定が正しくない。	N行目のパラメータの設定を確認してください。
invalid time value(Y)	時間(Y)の設定が正しくない。	N行目の設定が範囲内(1～65000)に収まる数字であるか確認してください。
symbol not found	分類キーワードが指定される前にキーワードが指定された。	キーワードは分類キーワードの後ろに設定する必要があります。N行目の設定を確認してください。
symbol[Y] already specified (ignored to line Z)	同じ分類キーワードYが複数設定されている。line Zまでは無視された。	2つ目以降の分類キーワードの設定は無効になりますので、N行目からの設定を確認してください。

■ ippool warningメッセージ

これは、起動時あるいはreloadコマンド実行時にippoolファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

ippool(line N):メッセージ

N：セットアップファイルの行番号

表B-27　Warningメッセージ一覧(ippool)

メッセージ	意　味	対　処
invalid count[Z] (the line ignored).	アドレスの数[Z]が不正のため、この行は無視された。	アドレスの数の指定を正しくしてください。10進数で512以下に指定してください。
invalid address[Z] (the line ignored).	アドレス[Z]が不正のため、この行は無視された。	アドレスの指定を正しくしてください。
invalid mask[Z] (the line ignored).	マスク[Z]が不正のため、この行は無視された。	マスクの指定を正しくしてください。
address[Z] already in use. ippool(line N):address[Z~] over.	アドレス[Z]がすでに使われている。	アドレスを他とぶつからないように指定してください。
	アドレス[Z]以降が数の上限(512個)を越えた。	アドレスは各プールごとに512個以内にしてください。
address[Z] not used.	アドレス[Z]は使用されなかった。	アドレスでホスト部が0になるような指定をしないでください。
address[Z] range over.	アドレス[Z]のレンジを越えた。	アドレスでホスト部の範囲を越えないようにしてください。

■ interface Warningメッセージ

これは、起動時あるいはreloadコマンド実行時にinterfaceファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

interface(line N):メッセージ

N：セットアップファイルの行番号
（行番号がない場合もあります）

表B-28　Warningメッセージ一覧(interface)

(1 / 3)

メッセージ	意　味	対　処
invalid broadcast argument, ignore this line.	ブロードキャストのアーギュメントが正しくない。 この行は無視された。	ブロードキャストの行の設定を確認してください。
invalid secondary argument, ignore this line.	正しくないsecondaryアーギュメントである。 この行は無視された。	N行目の2番目のアーギュメントを確認してください。
undefined filter, ignore this line.	定義されていないフィルタである。 この行は無視された。	指定したフィルタがipfiltersファイルで定義されているか確認してください。
filter already specified, ignore this line.	フィルタがすでに指定してある。 この行は無視された。	filter行を複数指定していないか確認してください。
unknown flag, ignore this line.	未定義のフラグである。 この行は無視された。	unnumbered、numbered、downなどの設定が正しいか確認してください。
unknown argument, ignore this line.	未定義のアーギュメントである。 この行は無視された。	N行目のアーギュメントを確認してください。
address required, ignore this line.	アドレスが必要である。 この行は無視された。	アドレスの指定をしてください。
filter name required, ignore this line.	フィルタ名が必要である。 この行は無視された。	フィルタ名を追加してください。
'include' or 'exclude' required, ignore this line.	'include'または'exclude'が必要である。 この行は無視された。	アクセスフィルタの設定を確認してください。
number required, ignore this line.	番号が必要である。 この行は無視された。	番号で指定してください。
no default address, ignore this line.	デフォルトアドレスがない。 この行は無視された。	デフォルトのアドレスを指定してください。
exceed broadcast address max (z), ignore this line.	ブロードキャストアドレスの最大個数(z)を越えている。 この行は無視された。	指定するブロードキャスト数を減らしてください。

表B-28　Warningメッセージ一覧(interface)

(2 / 3)

メッセージ	意　味	対　処
value range error, ignore this line.	指定した値が範囲外である。 この行は無視された。	設定した値の範囲を確認してください。
invalid argument, ignore this interface.	正しくないアーギュメントである。 このインタフェースは無視された。	N行目のアーギュメントを確認してください。
hostname invalid or unknown, ignore this interface.	ホスト名が正しくないか未定義である。 このインタフェースは無視された。	ホスト名を確認してください。また、hostsファイルに登録されているか確認してください。
invalid prefix specification, ignore this interface.	正しくないprefix設定である。 このインタフェースは無視された。	N行目のマスクの設定を確認してください。
interface-specifier invalid, ignore this interface.	論理インタフェース名が正しくない。 このインタフェースは無視された。	N行目の論理インタフェース名を確認してください。
invalid destination, ignore this interface.	正しくないデスティネーションである。 このインタフェースは無視された。	N行目のデスティネーションの設定を確認してください。
prefix-specifier required, ignore this interface.	prefix-specifierが必要である。 このインタフェースは無視された。	N行目のマスクの設定を確認してください。
'on' or 'off' required, ignore this interface.	'on'または'off'が必要である。 このインタフェースは無視された。	'on'または'off'を指定してください。
number required, ignore this interface.	番号が必要である。 このインタフェースは無視された。	番号で指定してください。
interface name required, ignore this interface.	論理インタフェース名が必要である。 このインタフェースは無視された。	論理インタフェース名を指定してください。
keyword 'interface' required, ignore this interface.	キーワード'interface'が必要である。 このインタフェースは無視された。	キーワード'interface'を指定してください。
invalid flag, ignore this interface.	正しくないフラグである。 このインタフェースは無視された。	unnumbered、numbered、downなどの設定が正しいか確認してください。
prefix specification range error, ignore this interface.	prefix設定のとりうる範囲外である。 このインタフェースは無視された。	マスクの設定を確認してください。
invalid cost, ignore this interface.	正しくない送信コストである。 このインタフェースは無視された。	コストの設定を確認してください。
gateway syntax error, ignore this interface.	ゲートウェイの構文エラーである。 このインタフェースは無視された。	N行目のゲートウェイの設定を確認してください。
syntax error, ignore this interface.	構文エラー。 このインタフェースは無視された。	N行目の設定を確認してください。

表B-28　Warningメッセージ一覧(interface)

(3 / 3)

メッセージ	意　味	対　処
couldn't find default local address.	default local addressを見つけられなかった。	hostnameファイルおよびhostsファイルの設定を確認してください。
couldn't install interface(X) setup.	論理インタフェース(X)の設定ができなかった。	interfaceファイルの論理インタフェース(X)の設定を確認してください。
reconfiguration fail(X).	論理インタフェース(X)の設定が失敗した。	interfaceファイルの論理インタフェース(X)の設定を確認してください。
reconfiguration fail.	再配置が失敗した。	interfaceファイル、gatewaysファイルの設定を確認してください。
couldn't install interface address.	インタフェースアドレスをインストールできなかった。	interfaceファイルの設定を確認してください。
multiple speed specified	phyサブキーワードでスピードが複数設定されている。	N行目の設定を確認してください。
line speed notsupported	phyサブキーワードのスピードの設定が不正である。	N行目の設定を確認してください。
invalid proxyarp argument, ignore this line	正しくないproxyarpアーギュメントである。 この行は無視された。	proxyarpのアーギュメントには、on_demandを指定してください。
'off' or 'auto' or 'all' required, ignore this line.	'off'、'auto'または'all'が必要である。 この行は無視された。	proxyarp on_demandには、'off'、'auto'または'all'を指定してください。

■ gateways Warningメッセージ

これは、起動時あるいはreloadコマンド実行時にgatewaysファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

gateways(line N):メッセージ

N：セットアップファイルの行番号
（行番号がない場合もあります）

表B-29　Warningメッセージ一覧(gateways)

(1 / 2)

メッセージ	意　味	対　処
underfined filter, ignore this line.	未定義なフィルタ名である。 この行は無視された。	フィルタ名を確認してください。また、ipfiltersファイルの設定を確認してください。
filter already specified, ignore this line.	フィルタはすでに指定してある。 この行は無視された。	フィルタ行が複数指定されていないか確認してください。
filter name required, ignore this line.	フィルタ名が必要である。 この行は無視された。	フィルタ名を指定してください。
syntax error, ignore this line.	構文エラー。 この行は無視された。	N行目を確認してください。
invalid argument, ignore this route.	正しくないアーギュメントである。 このルートは無視された。	N行目のアーギュメントを確認してください。
hostname invalid or unknown, ignore this route.	ホスト名が正しくないか未定義である。 このルートは無視された。	ホスト名が正しいか確認してください。また、hostsファイルに登録されているか確認してください。
invalid prefix specification, ignore this route.	正しくないprefix設定である。 このルートは無視された。	マスクの設定を確認してください。
interface-specifier invalid, ignore this route.	論理インタフェース名が正しくない。 このルートは無視された。	論理インタフェース名の指定を確認してください。
invalid option, ignore this route.	正しくないオプションである。 このルートは無視された。	N行目の設定を確認してください。
prefix-specifier required, ignore this route.	prefix-specifierが必要である。 このルートは無視された。	マスクの設定を確認してください。
'on' or' off' required, ignore this route.	'on'または'off'が必要である。 このルートは無視された。	'on'または'off'で指定してください。
number required, ignore this route.	番号が必要である。 このルートは無視された。	番号で指定してください。
destination address required, ignore this route.	宛先アドレスが必要である。 このルートは無視された。	宛先アドレスを指定してください。

表B-29　Warningメッセージ一覧(gateways)

(2 / 2)

メッセージ	意　味	対　処
'via' required, ignore this route.	キーワード'via'が必要である。このルートは無視された。	キーワード'via'を指定してください。
gateway required, ignore this route.	ゲートウェイが必要である。このルートは無視された。	ゲートウェイを指定してください。
keyword 'destination' required, ignore thisroute.	キーワード'destination'が必要である。このルートは無視された。	キーワード'destination'を指定してください。
prefix specification range error, ignore this route.	prefix設定のとりうる範囲外である。このルートは無視された。	マスクの設定を確認してください。
invalid cost, ignore this route.	正しくない送信コストである。このルートは無視された。	コストの設定を確認してください。
cost range error (1~99), ignore this route.	送信コストが1～99の範囲外である。	コストの設定を確認してください。
gateway syntax error, ignore this route.	ゲートウェイの構文エラー。このルートは無視された。	N行目の設定を確認してください。
syntax error, ignore this route.	構文エラー。このルートは無視された。	N行目の設定を確認してください。
couldn't install the route (z).	zから始まるrouteがインストールできなかった。	gatewaysファイルの設定を確認してください。

■ snmpd:snmpconf Warningメッセージ

これは、snmpconfファイルの解析に関するWarningメッセージです。

表B-30　Warningメッセージ一覧(snmpd:snmpconf)

メッセージ	意　味	対　処
snmpd: snmpconf NG syntax (**X**): too long line	(X)行目の行が長すぎる。	1行の長さを短くしてください。
snmpd: snmpconf NG syntax (**X**): illegal argument	(X)行目のアーギュメントの数が正しくないか、設定値が誤っている。	正しいアーギュメントの指定してください。
snmpd: snmpconf NG syntax (**X**): unknown host	(X)行目で設定されたホスト名のIPアドレスが見つからない。	設定したホスト名が正しいか、hostsファイルに登録されているか確認してください。DNSを使用している場合には、DNSサーバのホストの設定を確認してください。
snmpd: snmpconf NG syntax (**X**): unknown keyword	(X)行目でキーワードの指定が誤っている。	正しいキーワードを指定してください。
snmpd: snmpconf (**X**): no such interface	(X)行目で指定したインタフェース名は存在しない。	インタフェース名を確認してください。
snmpd: snmpconf NG syntax (**X**): over maximum use times	(X)行目でキーワードの繰り返し使用の回数が制限を越えた。	そのキーワードの使用回数を減らしてください。

■ rip.conf Warningメッセージ

これは、rip.confファイルの解析に関するWarningメッセージです。
次のようなフォーマットになっています。

rip.conf(line N): メッセージ

N：セットアップファイルの行番号
（行番号がない場合もあります）

表B-31　Warningメッセージ一覧(rip.conf)

メッセージ	意　味	対　処
unknown keyword[X]	キーワード[X]が正しくない。	N行目のキーワードの設定を確認してください。
invalid interface[X]	論理インタフェース[X]が正しくない。	設定した論理インタフェース名が正しいか確認してください。
no such interface[X]	論理インタフェース[X]が存在しない。	設定した論理インタフェース名が正しいか確認してください。
invalid interface keyword [X]	論理インタフェースのキーワード[X]が正しくない。	N行目の論理インタフェースのキーワードの設定を確認してください。
invalid value at interface in/out [X]	論理インタフェースの送受信の設定[X]が正しくない。	論理インタフェースの送受信の設定を確認してください。
invalid authentication use	認証の使用の設定が正しくない。	認証の使用の設定を確認してください。
password is too long	パスワードが長すぎる。	パスワードを16文字以下に設定してください。
not set authentication password	認証のパスワードが設定されていない。	パスワードを設定してください。
invalid destination address [X]	宛先アドレス[X]が正しくない。	設定した宛先アドレスを確認してください。
netmask required	マスクの設定が必要である。	マスクを設定してください。
invalid gateway address [X]	ゲートウエイアドレス[X]が正しくない。	設定したゲートウエイアドレスを確認してください。
unreachable gateway[X]	指定されたゲートウエイは到達できない。	到達可能なゲートウエイを指定してください。
invalid metric[X]	メトリック[X]が正しくない。	メトリックを1から15までの10進数で設定してください。
this route[dst:X] already exist	このルート[宛先:X]はすでに存在する。	設定したルートを確認してください。
missing value for keyword [X]	キーワード[X]に対して引数がない。	キーワード[X]に対する引数を設定してください。

■ **syslog.conf Warningメッセージ**

これは、起動時あるいはreloadコマンド実行時にsyslog.confファイルを解析した時に出力されるWarningメッセージです。
次のようなフォーマットになっています。

syslog.conf(line N): メッセージ

N：セットアップファイルの行番号
（行番号がない場合もあります）

表B-32　Warningメッセージ一覧(syslog.conf)

メッセージ	意　　味	対　　処
unknown keyword,ignore this line.	正しくないキーワードが指定された。 この行は無視された。	N行目のキーワードの設定を確認してください。
invalid parameter,ignore this line.	正しくないパラメータが指定された。 この行は無視された。	N行目のパラメータの設定を確認してください。
'host' required,ignore this configuration.	hostキーワードの設定が必要である。 このSYSLOGの設定は無視された。	hostキーワードの設定を確認してください。
'facility' required, ignore this configuration.	facilityキーワードの設定が必要である。 このSYSLOGの設定は無視された。	facilityキーワードの設定を確認してください。

B.4　トレースメッセージの表示方法

トレースメッセージとは、本装置の通信状況を表示するメッセージです。トレースメッセージは、本装置のコンソール、あるいはあらかじめ設定されているsyslogホストに出力することができます。

(1) トレースメッセージの種類

トレースメッセージには、**表B-33**に示すカテゴリがあります。それぞれのカテゴリごとに本装置のコンソールあるいはあらかじめ設定されているsyslogホストにメッセージを出力することができます。

表B-33　トレースメッセージのカテゴリ

カテゴリ	トレースメッセージの内容
ISDN	ISDN呼制御の接続／切断
PPP	PPPの接続／切断
SESSION	セッションの確立／切断
RADIUS	RADIUSサーバとの通信
DSP	モデム／PIAFSの接続／切断

(2) 本装置のコンソールにトレースメッセージを出力する方法

本装置のコンソールにトレースメッセージを出力する場合、トレースメッセージのカテゴリごとに用意されているコマンド（**表B-34**参照）を実行します。

表B-34　トレースメッセージを制御するコマンド

カテゴリ	トレースメッセージを制御するコマンド
ISDN	isdntrace on｜off
PPP	ppptrace on｜off
SESSION	sessiontrace on｜off
RADIUS	radiustrace on｜off
DSP	dsptrace on｜off

各コマンドとも、パラメータには「on」と「off」があります。「on」を指定すると、以後そのカテゴリのトレースメッセージが本装置のコンソールに表示されます。また「off」を指定すると、表示されなくなります。

カテゴリ：SESSIONのトレースメッセージを本装置のコンソールに表示する場合

```
# sessiontrace  on
```
（以後本装置のコンソールにカテゴリ：SESSIONのトレースメッセージが表示されます）

(3) syslogでトレースメッセージを出力する方法

syslogでトレースメッセージを出力する場合には、syslog.confファイルを設定する必要があります。syslog.confファイルの設定方法の詳細は**「5.15　syslog.confファイル」**を参照してください。
各カテゴリのトレースメッセージをsyslogで出力する場合、以下の例のように出力したいカテゴリを示すキーワードを、「on」に設定します。

カテゴリ：SESSIONをsyslogに出力する場合のsyslog.confファイルの設定例

```
sessiontrace      on
```

B.5　トレースメッセージの見方

(1) 本装置のコンソールに出力されるトレースメッセージのフォーマット

本装置のコンソールに出力されるトレースメッセージは、以下のようなフォーマットで表示されます。

```
@T(8/30 12.50.13):[CID 4016]:session(7008864):UP(1) sii C1-4-19 PIAFS(V2.1) PPP 172.31.11.61 tel=
```

日付と時刻　CID　カテゴリ　メッセージ

日付と時刻

：トレースメッセージのイベントが発生した日付と時刻が表示されます。メッセージによっては表示されないものがあります。

CID

：ISDN回線を使用した場合は、通信の開始から終了までの間で関連する複数のモジュールに渡ってユニークになるIDが表示されます。
カテゴリが、ISDN、PPP、SESSIONおよびDSPの場合に表示され、RADIUSの場合には、表示されません。
高速ディジタル回線を使用した場合は、以下のように表示されます。
カテゴリが、PPP、SESSIONの場合に表示されます。

[CID xyyy]

x　：高速ディジタル回線で使用しているPRIボードのPRIポート番号(1～6)
yyy　：PRIポート内の論理チャネル番号(001～024)
　boardsファイルの%channelで設定した論理チャネル番号

カテゴリ

：トレースメッセージのカテゴリが表示されます。

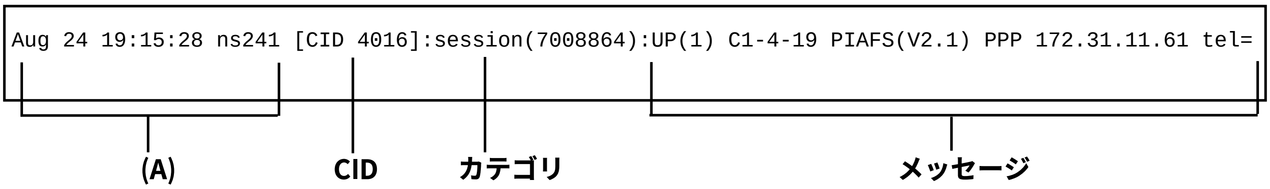
メッセージ

：それぞれのカテゴリに対応したメッセージが表示されます。

表示されるメッセージの内容については、**「B.6　トレースメッセージのフォーマット」**を参照してください。

(2) syslogで出力されるトレースメッセージのフォーマット

本装置からトレースメッセージを受信したsyslogホストにおける表示は、そのホストのsyslogの仕様に依存しますが、一般的には、以下のようなフォーマットで表示されます。



(A)
： この部分は、syslogメッセージを受信したホストが挿入します。

CID
： ISDN回線を使用した場合は、通信の開始から終了までの間で複数のモジュールに渡ってユニークになるIDが表示されます。
カテゴリが、ISDN、PPP、SESSIONおよびDSPの場合に表示され、RADIUSの場合には、表示されません。
高速ディジタル回線を使用した場合は、以下のように表示されます。
カテゴリが、PPP、SESSIONの場合に表示されます。

[CID xyyy]

x ：高速ディジタル回線で使用しているPRIボードのPRIポート番号(1～6)
yyy ：PRIポート内の論理チャネル番号(001～024)
boardsファイルの%channelで設定した論理チャネル番号

カテゴリ
： トレースメッセージのカテゴリが表示されます。

メッセージ
： それぞれのカテゴリに対応したメッセージが表示されます。

表示されるメッセージの内容は、**「B.6　トレースメッセージのフォーマット」**を参照してください。

B.6　トレースメッセージのフォーマット

トレースメッセージは、本装置のコンソールに出力される場合と、あらかじめ設定されているsyslogホストに出力される場合と、メッセージ本体は同様の内容です。ただし、メッセージ本体の前に挿入されるヘッダは、異なるので、**「B.5　トレースメッセージの見方」**を参照してください。

また、syslogを使用するように設定している場合には、本装置の起動時に、以下のメッセージがsyslogホストに出力されます。

```
Dec  5 17:10:48 ns241 boot:Multiservice Platform NS-4200-10 System
Software 2001.xx.xx (Ver X.X)
```

この内容は、本装置の製品の型式と、システムソフトウェアのバージョン（日付およびバージョン番号）を表しています。バージョンの部分は、バージョンによって変化します。

以下にトレースメッセージの各カテゴリごとに、表示されるメッセージのフォーマットについて説明します。

■ISDNトレースメッセージ

これは、主にISDN呼制御の接続／切断に関するトレースメッセージです。
ISDNトレースメッセージは、さらに以下のものに分類されます。

・CCトレースメッセージ
・PHトレースメッセージ

(1) 表示例

本装置のコンソールに表示されるトレースメッセージの表示例を以下に示します。

ISDN呼の接続(着呼)から切断(接続相手からの切断)までのトレースメッセージの表示例

```
@T(12/5 11.31.33):[CID 4016]:CC:P1-4:InConnect(CS[PIAFS(V2.1)],8010,0123456789,B19)
@T(12/5 11.31.56):[CID 4016]:CC:P1-4:DiscInd(CS[PIAFS(V2.1)],8010,0123456789,B19,T23,
C-,normal(#16,0))
```

ISDN呼の接続(発呼)から切断(本装置からの切断)までのトレースメッセージの表示例

```
@T(12/5 11.38.30):[CID 4017]:CC:P1-4:OutConnect(CS[PIAFS(V2.1)],4f,0123456789,B19)
@T(12/5 11.39.22):[CID 4017]:CC:P1-4:DiscReq(CS[PIAFS(V2.1)],4f,0123456789,B19,T52,
C10,send(#16,0))
```

ISDNのlayer1が確立したときのトレースメッセージの表示例

```
@T(12/5 18.1.29):PH:P1-4:Layer1 UP
```

ISDNのlayer1が切断したときのトレースメッセージの表示例

```
@T(12/5 18.1.35):PH:P1-4:Layer1 DOWN
```

(2) CCトレースメッセージのフォーマット

CCトレースメッセージは、ISDN呼制御の接続／切断を表示します。
CCトレースメッセージには、以下の4種類のメッセージがあります。

[CID ****]:CC:Px-y:InConnect(P1,P2,P3,P4)
[CID ****]:CC:Px-y:OutConnect(P1,P2,P3,P4)
[CID ****]:CC:Px-y:DiscInd(P1,P2,P3,P4,P5,P6,P7)
[CID ****]:CC:Px-y:DiscReq(P1,P2,P3,P4,P5,P6,P7)

各トレースメッセージのパラメータの意味は、以下のとおりです。

Px-y

： PRIボードのスロット番号／ポート番号

x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号

InConnect

： ISDNの呼が着信により接続したことを示します。

OutConnect

： ISDNの呼が発信により接続したことを示します。

DiscInd

： ISDNの呼が接続相手から切断されたことを示します。

DiscReq

： ISDNの呼を本装置から切断したことを示します。

P1

： 回線サービス種別

CS	：回線交換(HDLC接続)
CS[PIAFS(V1.0)]	：回線交換(PIAFS(V1.0)接続)
CS[PIAFS(V2.0)]	：回線交換(PIAFS(V2.0)接続)
CS[PIAFS(V2.1)]	：回線交換(PAIFS(V2.1)接続)
CS[MODEM]	：回線交換(モデム接続)

P2

： ISDN呼制御プロトコル上の呼番号が表示されます。
16進数で表示されます。

P3

： 相手電話番号が表示されます。
サブアドレスがある場合は、*(アスタリスク)で区切られた後に表示されます。

P4

： Bチャネル番号が表示されます。

P5

： この呼が接続していた時間(秒)を示します。
例えば、接続時間が67秒の場合、T67のように表示されます。

P6

： 網から通知された通信料金を示します。
例えば、通信料金が10円の場合、C10のように表示されます。

P7

： ISDN呼制御プロトコル上の理由表示(TTC標準JT-Q850で規定されている)を示します。
例えば、normal(#16,0)のように表示されます。カッコ内は、#<理由表示値>, <生成源>のようなフォーマットになっており、この例では、理由表示値が16、生成源が0です。

(3) PHトレースメッセージのフォーマット

PHトレースメッセージは、ISDN回線のLayer1の確立／切断に関連するトレースメッセージで、以下の2種類のメッセージがあります。

PH:Px-y:Layer1 UP
PH:Px-y:Layer1 DOWN

各トレースメッセージのパラメータの意味は、以下のとおりです。

Px-y

： PRIボードのスロット番号／ポート番号

x ：Layer1が確立／切断したPRIボードのスロット番号
y ：Layer1が確立／切断したPRIボードのPRIポート番号

Layer1 UP

： ISDN回線のLayer1が確立したことを示します。

Layer1 DOWN

： ISDN回線のLayer1が切断したことを示します。

■ PPPトレースメッセージ

これは、主にPPPのネゴシエーションに関連するトレースメッセージです。
このメッセージはプロトコル別に以下の６種類に分類されています。

- ・LCPトレースメッセージ
- ・LCP Bindトレースメッセージ
- ・CBCPトレースメッセージ
- ・BACPトレースメッセージ
- ・BAPトレースメッセージ
- ・NCPトレースメッセージ

(1) 表示例

本装置のコンソールに表示されるトレースメッセージの表示例を以下に示します。

PPP接続の接続から切断までのトレースメッセージの表示例

```
@T(12/5 11.31.34):[CID 4016]:LCP(C1-4-19)::UP[PPP](MRU:1524/1500)(ACCM:0x0/0xa0000)
(AUTH:CHAP/NONE)(MN:0x0/0x8715aae4)(PFC:OFF/OFF)(ACFC:OFF/OFF)(CB:CBCP)
@T(12/5 11.31.35):[CID 4016]:LCP(C1-4-19):sii:Bind(BUNDLE:183)(LINK:1)
@T(12/5 11.31.35):[CID 4016]:CBCP(C1-4-19):sii:[NoCallback]
@T(12/5 11.31.35):[CID 4016]:NCP(183):sii:UP(192.168.0.1/10.0.0.1)
@T(12/5 11.31.56):[CID 4016]:LCP(C1-4-19):sii:DOWN
@T(12/5 11.31.56):[CID 4016]:LCP(C1-4-19):sii:UnBind(BUNDLE:183)(LINK:0)
@T(12/5 11.31.56):[CID 4016]:NCP(183):sii:DOWN(0:00:21,in=10,out=10)
```

BACP接続の接続から切断までのトレースメッセージの表示例

```
@T(12/5 11.32.21):[CID 4017]:LCP(C1-4-19)::UP[BACP](MRU:1524/1500)(ACCM:0x0/0xa0000)
(AUTH:CHAP/NONE)(MN:0x0/0x874486b2)(PFC:OFF/OFF)(ACFC:OFF/OFF)(CB:CBCP)(MRRU:1524/1500)
(ED:MAC,08008375880d/LOCAL,4255475f0ae4dbaf)(LD:0x401/0dbaf)
@T(12/5 11.32.22):[CID 4017]:LCP(C1-4-19):sii:Bind(BUNDLE:183)(LINK:1)
@T(12/5 11.32.22):[CID 4017]:CBCP(C1-4-19):sii:[NoCallback]
@T(12/5 11.32.22):[CID 4017]:BACP(183):sii:UP(FAVORED:0xffffffff/0xae4dbe4)
@T(12/5 11.32.22):[CID 4017]:NCP(183):sii:UP(192.168.0.1/10.0.0.1)
@T(12/5 11.32.27):[CID 4017]:BAP(183):sii:[InCallReq:ACK](NoPhone)
@T(12/5 11.32.30):[CID 4018]:LCP(C1-4-20)::UP[BACP](MRU:1524/1500)(ACCM:0x0/
0xa0000)(AUTH:CHAP/NONE)(MN:0x0/0x874cb161)(PFC:OFF/OFF)(ACFC:OFF/OFF)(CB:CBCP)(MRRU:1524/
1500)(ED:MAC,08008375880d/LOCAL,4255475f0ae4dbaf)(LD:0x402/0xdbb0)
@T(12/5 11.32.30):[CID 4018]:LCP(C1-4-20):sii:Bind(BUNDLE:183)(LINK:2)
@T(12/5 11.32.30):[CID 4018]:CBCP(C1-4-20):sii:[NoCallback]
@T(12/5 11.32.51):[CID 4018]:LCP(C1-4-20):sii:DOWN
@T(12/5 11.32.51):[CID 4017]:LCP(C1-4-19):sii:DOWN
@T(12/5 11.32.52):[CID 4018]:LCP(C1-4-20):sii:UnBind(BUNDLE:183)(LINK:1)
@T(12/5 11.32.52):[CID 4017]:LCP(C1-4-19):sii:UnBind(BUNDLE:183)(LINK:0)
@T(12/5 11.32.52):[CID 4017]:BACP(183):sii:DOWN
@T(12/5 11.32.52):[CID 4017]:NCP(183):sii:DOWN(0:00:30,in=10,out=10)
```

(2) LCPトレースメッセージのフォーマット

LCPトレースメッセージは、PPPのうちLCP（Link Control Protocol）のネゴシエーションに関連するトレースメッセージで、以下の3種類のメッセージがあります。

[CID ****]:LCP(P1):P2:UP[プロトコル](オプション)(オプション)・・・
[CID ****]:LCP(P1):P2:DOWN
[CID ****]:LCP(P1):P2:RESET

各トレースメッセージのパラメータの意味は、以下のとおりです。

P1

：識別情報を示します。

・NS-4200-10の場合
(Cw-x-y-z)
w ：PPP(LCP)が動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：ISDN回線の場合は発着信したPRIポートのBチャネル番号
高速ディジタル回線の場合はPRIポート内の論理チャネル番号で、boardsファイルの%channelで設定した論理チャネル番号

・NS-4200-30の場合
(Cx-y-z)
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

P2

：相手局ユーザ名が表示されます。ただしユーザ名が特定できない場合は表示されません。

UP

：LCPが接続したことを示します。

DOWN

：LCPが切断したことを示します。

RESET

：LCPが再度ネゴシエーションされたことを示します。

プロトコル

：LCPのネゴシエーションで成立したプロトコルを示します。
PPP ：ネゴシエーションの結果PPPで接続した
MP ：ネゴシエーションの結果MPで接続した
BACP ：ネゴシエーションの結果BACPで接続した

オプション

：LCPのネゴシエーションで成立した主なオプションとその値が表示されます。（**表B-35** 参照）

表B-35　LCPトレースメッセージのオプション

(1 / 2)

オプション	意　味
MRU:x/y	MRU（Maximum Received Unit）は、1パケットで受信可能な最大サイズを示します。 x：自局が相手局に通知した自局のMRU値 y：相手局が自局に通知した相手局のMRU値
ACCM:x/y	ACCM（Async Control Character Map）は、受信したフレームを非同期／同期変換する際に使用する制御キャラクタマップを示します。 x：自局が相手局に通知した自局のACCM値 y：相手局が自局に通知した相手局のACCM値
AUTH:x/y	AUTH（Authentication）は、PPP認証で使用する認証プロトコルを示します。 x：自局が相手局を認証するプロトコル y：相手局が自局を認証するプロトコル x、yで示される内容は以下の3つがあります。 NONE：認証しない PAP　：PAPで認証する CHAP：CHAPで認証する
MN:x/y	MN（Magic Number）は、自局と相手局を区別するための識別子を示します。 x：自局が相手局に通知した自局のMN値 y：相手局が自局に通知した相手局のMN値
PFC:x/y	PFC（Protocol Field Compression）は、プロトコルフィールドを圧縮したパケットが受信可能かどうかを示します。 x：自局が相手局に通知したPFC y：相手局が自局に通知したPFC x、yで示される内容は以下の2つがあります。 OFF　：プロトコルフィールドを圧縮したパケットは受信不可 ON　：プロトコルフィールドを圧縮したパケットは受信可能

表B-35　LCPトレースメッセージのオプション

(2 / 2)

オプション	意　味
ACFC:x/y	ACFC（Address and Control Field Compression）は、アドレスおよびコントロールフィールドを圧縮したパケットが受信可能かどうかを示します。 x：自局が相手局に通知したACFC y：相手局が自局に通知したACFC x、yで示される内容は以下の2つがあります。 OFF：アドレスおよびコントロールフィールドを圧縮したパケットは受信不可 ON ：アドレスおよびコントロールフィールドを圧縮したパケットは受信可能
CB:x	CB（Callback）は、コールバックのネゴシエーションで使用するプロトコルを示します。 xで示される内容は以下の2つがあります。 NONE：コールバックのネゴシエーションを行わない CBCP ：CBCPを使用してネゴシエーションを行う
MRRU:x/y	MRRU（Maximum Received Reconstructed Unit）は、再構築されたMPパケットで受信可能な最大サイズを示します。 MPまたはBACPで使用されます。 x：自局が相手局に通知した自局のMRRU値 y：相手局が自局に通知した相手局のMRRU値
ED:x/y	ED（Endpoint Discriminator）は、各装置固有の識別子を示します。 MPまたはBACPで使用されます。 x：自局が相手局に通知した自局のED y：相手局が自局に通知した相手局のED この値は装置固有の識別子のため、よくMACアドレスが使用されます。 本装置もMACアドレスを使用しています。
LD:x/y	LD（Link Discriminator）は、BACP接続で使用するリンクごとの識別子を示します。 x：自局が相手局に通知した、このリンクのLD y：相手局が自局に通知した、このリンクのLD

(3) LCP Bindトレースメッセージのフォーマット

LCP Bindトレースメッセージは、PPPのLCPとNCPの関連付けについてのトレースメッセージで、以下の2種類のメッセージがあります。

[CID ****]:LCP(P1):P2:Bind(BUNDLE:N1)(LINK:N2)
[CID ****]:LCP(P1):P2:UnBind(BUNDLE:N1)(LINK:N2)

各トレースメッセージのパラメータの意味は、以下のとおりです。

P1

：識別情報を示します。

・NS-4200-10の場合
(Cw-x-y-z)
w ：PPP(LCP)が動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：ISDN回線の場合は発着信したPRIポートのBチャネル番号
高速ディジタル回線の場合はPRIポート内の論理チャネル番号で、boardsファイルの%channelで設定した論理チャネル番号

・NS-4200-30の場合
(Cx-y-z)
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

P2

：相手局ユーザ名が表示されます。ただしユーザ名が特定できない場合は表示されません。

Bind

：LCPとNCPが関連付けられたことを示します。

UnBind

：LCPとNCPの関連付けが解消されたことを示します。

N1

：このLCPと関連付けられた（または関連付けが解消された）NCPの識別番号が表示されます。

N2

：Bind/UnBind後に、このNCPと関連付けられているLCPの数が表示されます。

(4) CBCPトレースメッセージのフォーマット

CBCPトレースメッセージは、PPPのうちCBCP（Callback Control Protocol）のネゴシエーションに関連するトレースメッセージで、以下の1種類のメッセージがあります。

[CID ****]:CBCP(P1):P2:[結果](オプション)(オプション)・・・

各トレースメッセージのパラメータの意味は、以下のとおりです。

P1

：識別情報を示します。

・NS-4200-10の場合
(Cw-x-y-z)
w ：CBCPが動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

・NS-4200-30の場合
(Cx-y-z)
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

P2

：相手局ユーザ名が表示されます。ただしユーザ名が特定できない場合は表示されません。

結果

：CBCPのネゴシエーションの結果を示します。

NoCallback	：コールバックを行わないことを示します。
Request	：自局のコールバック要求が相手局に受け入れられたことを示します。
Accept	：相手局のコールバック要求を自局が受け入れたことを示します。

オプション

：CBCPのネゴシエーションで成立したオプションとその値が表示されます。（**表B-36**参照）

表B-36　CBCPトレースメッセージのオプション

オプション	意　味
TYPE:x	TYPE（Callback Type）は、コールバックする電話番号のタイプを示します。 xで示される内容は以下の2つがあります。 AdminNumber ：コールバック要求を受け入れた側で設定された電話番号 UserNumber=y：コールバック要求を行う側で指定した電話番号(y)
DELAY:x	DELAY（Delay Time）は、コールバックを行うまでのディレイ時間を示します。 x：コールバック要求を行う側で指定したディレイ時間（単位：秒）

(5) BACPトレースメッセージのフォーマット

BACPトレースメッセージは、PPPのうちBACP（Bandwidth Allocation Control Protocol）のネゴシエーションに関連するトレースメッセージで、以下の3種類のメッセージがあります。

[CID ****]:BACP(X):ユーザ名:UP(オプション)(オプション)・・・
[CID ****]:BACP(X):ユーザ名:DOWN
[CID ****]:BACP(X):ユーザ名:RESET

各トレースメッセージのパラメータの意味は、以下のとおりです。

X
：NCPの識別番号が表示されます。

ユーザ名
：相手局ユーザ名が表示されます。

UP
：BACPが接続したことを示します。

DOWN
：BACPが切断したことを示します。

RESET
：BACPが再度ネゴシエーションされたことを示します。

オプション

：BACPのネゴシエーションで成立したオプションとその値が表示されます。（**表B-37** 参照）

表B-37　BACPトレースメッセージのオプション

オプション	意　味
FAVORED:x/y	FAVORED（Favored-Peer）は、要求が競合した場合に優先される側を決める値を示します。 x：自局が相手局に通知した自局側の値 y：相手局が自局に通知した相手局側の値 競合した場合は、値の小さい側の要求が優先されます。

(6) BAPトレースメッセージのフォーマット

BAPトレースメッセージは、PPPのうちBAP（Bandwidth Allocation Protocol）のネゴシエーションに関連するトレースメッセージで、以下の1種類のメッセージがあります。

[CID ****]:BAP(X):ユーザ名:[要求内容:結果](オプション)(オプション)・・・

各トレースメッセージのパラメータの意味は、以下のとおりです。

X

：NCPの識別番号が表示されます。

ユーザ名

：相手局ユーザ名が表示されます。

要求内容

：BAPによる帯域制御要求の内容を示します。

InCallReq	：発信によるリンク追加要求が相手局から要求されたことを示します。
OutCallReq	：発信によるリンク追加要求を相手局へ要求したことを示します。
InCallbackReq	：コールバックによるリンク追加要求が相手局から要求されたことを示します。
OutCallbackReq	：コールバックによるリンク追加要求を相手局へ要求したことを示します。
InLinkDropReq	：リンク切断要求が相手局から要求されたことを示します。
OutLinkDropReq	：リンク切断要求を相手局へ要求したことを示します。

結果

：BAPによる帯域制御要求の結果を示します。

ACK　　：要求を受け入れたことを示します。
NAK　　：一時的な要因で要求を拒否したことを示します。
FullNAK ：受け入れ可能な範囲を超えるため要求を拒否したことを示します。
REJ　　：受け入れられない要求のため拒否したことを示します。

オプション

：BAPのネゴシエーションで成立した主なオプションとその値が表示されます。（**表B-38**参照）

表B-38　BAPトレースメッセージのオプション

オプション	意　味
Phone:x:y	Phone（Phone Delta）は、リンクの追加時に発信する電話番号を示します。 x：発信する電話番号のうち以前と異なる電話番号の桁数 y：発信する電話番号
NoPhone	NoPhone（No Phone Number Needed）は、リンクの追加要求時に電話番号のネゴシエーションが不要だったことを示します。
LD:x	LD（Link Discriminator）は、リンクの切断要求時に切断するリンクの識別子を示します。 x：切断するリンクの相手側のLD

(7) NCPトレースメッセージのフォーマット

NCPトレースメッセージは、PPPのうちNCP（Network Control Protocol）のネゴシエーションに関連するトレースメッセージで、以下の2種類のメッセージがあります。

[CID ****]:NCP(X):ユーザ名:UP(オプション)(オプション)・・・
[CID ****]:NCP(X):ユーザ名:DOWN(接続時間,in=a,out=b)

各トレースメッセージのパラメータの意味は、以下のとおりです。

X

：NCPの識別番号が表示されます。

ユーザ名

：相手局ユーザ名が表示されます。

UP

：NCPが接続したことを示します。

DOWN

：NCPが切断したことを示します。

オプション

：NCPのネゴシエーションで成立した主なオプションとその値が表示されます。（**表B-39**参照）

接続時間

：UPからDOWNまでの接続時間（単位：時：分：秒）が表示されます。

a

：UPからDOWNまでの受信パケット数が表示されます。

b

：UPからDOWNまでの送信パケット数が表示されます。

表B-39　NCPトレースメッセージのオプション

オプション	意　味
x/y	ネゴシエーションを行ったIPアドレスを示します。 x：自局のIPアドレス y：相手局のIPアドレス IPアドレスのネゴシエーションが行われなかった場合は - となります。

■ SESSIONトレースメッセージ

これは、セッションの確立／切断に関連するトレースメッセージです。

(1) 表示例

本装置のコンソールに表示されるトレースメッセージの表示例を以下に示します。

セッションの確立と切断のトレースメッセージの表示例

```
@T(12/5 11.31.35):[CID 4016]:session(3600028f):UP(1)   sii C1-4-19 PIAFS(V2.1) PPP 10.0.0.1
tel=07012345678
@T(12/5 11.31.56):[CID 4016]:session(3600028f):DOWN(1) sii C1-4-19 PIAFS(V2.1) PPP 10.0.0.1
tel=07012345678 time=21
@T(12/5 11.31.56):[CID 4016]:session(3600028f):STOP(45)
```

(2) トレースメッセージのフォーマット

セッションのトレースメッセージには、以下の3種類のメッセージがあります。

[CID ****]:session(SID):UP(N1) ユーザ名 P1 属性 プロトコル IPアドレス tel=電話番号
[CID ****]:session(SID):DOWN(N2) ユーザ名 P1 属性 プロトコル IPアドレス tel= 電話番号 time=接続時間
[CID ****]:session(SID):STOP(N3)

各トレースメッセージのパラメータの意味は、以下のとおりです。

SID
： セッションIDが表示されます。

UP
： セッションが確立したことを示します。

DOWN
： セッション確立後、セッションが切断したことを示します。

STOP
： セッションの確立前、確立後に関わらず、セッションの処理が終了したことを示します。

N1
： 接続が行われた方向を示します。

1　：着信
2　：発信（コールバックを除く）
3　：コールバックによる発信

N2

：セッション確立後の切断理由を示します。
詳細は**付録C**の**表C-3**（RADIUSアカウントサーバへ送信するattributeの内容）のAcct-Terminate-Causeの切断理由を参照してください。

N3

：セッション確立失敗または確立後の切断理由を示します。
詳細は**付録C**の**表C-3**（RADIUSアカウントサーバへ送信するattributeの内容）のAcct-Disconnect-Causeの切断理由を参照してください。

ユーザ名

：相手局ユーザ名が表示されます。

P1

：識別情報を示します。

・NS-4200-10の場合
(Cw-x-y-z)
w ：PPPが動作している拡張ボード(PRIまたはDSPボード)のスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：ISDN回線の場合は発着信したPRIポートのBチャネル番号
高速ディジタル回線の場合はPRIポート内の論理チャネル番号で、boardsファイルの%channelで設定した論理チャネル番号

・NS-4200-30の場合
(Cx-y-z)
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのPRIポート番号
z ：発着信したPRIポートのBチャネル番号

属性

：接続した回線の属性を示します。

MODEM(V32BIS)	：モデム（キャリアプロトコルV32bis）で接続
MODEM(V34)	：モデム（キャリアプロトコルV34）で接続
MODEM(K56F)	：モデム（キャリアプロトコルK56f）で接続
MODEM(V90)	：モデム（キャリアプロトコルV90）で接続
MODEM(OTHER)	：モデム（その他のキャリアプロトコル）で接続
PIAFS(V1.0)	：PIAFS V1.0で接続
PIAFS(V2.0)	：PIAFS V2.0で接続
PIAFS(V2.1)	：PIAFS V2.1で接続
HDLC	：HDLCで接続

プロトコル

： 接続したプロトコルを示します。

PPP　：PPPで接続
MP　：MPで接続
BACP：BACPで接続

IPアドレス

： 相手のIPアドレスが表示されます。
（IPアドレスのネゴシエーションが行われなかった場合は 0.0.0.0 になります）

電話番号

： 相手の電話番号が表示されます。
（相手から電話番号の通知がない場合や高速ディジタル回線の場合は空欄になります）

接続時間

： UPからDOWNまでの接続時間（単位：秒）が表示されます。

■ RADIUSトレースメッセージ

これは、RADIUSサーバとの通信に関連するトレースメッセージです。
RADIUSトレースメッセージは、以下の2種類に分類されます。

・radiusdトレースメッセージ
・acctdトレースメッセージ

(1) 表示例

本装置のコンソールに表示されるトレースメッセージの表示例を以下に示します。

radiusd 認証パケットのトレースメッセージの表示例

```
@T(8/29 16.8.5):radiusd:REQ:27,83(172.31.1.1)(sii)
@T(8/29 16.8.5):radiusd:ACT:27,38(172.31.1.1) 8 ms
```

acctd アカウントパケットのトレースメッセージの表示例

```
@T(8/29 16.8.5):acctd:REQ:61,123(172.31.1.1)(START,sii)
@T(8/29 16.8.6):acctd:RSP:61,139(172.31.1.1) 40 ms
@T(8/29 16.8.18):acctd:REQ:62,159(172.31.1.1)(STOP,sii)
@T(8/29 16.8.18):acctd:RSP:62,175(172.31.1.1) 46 ms
```

(2) radiusd トレースメッセージのフォーマット

radiusd トレースメッセージは、認証時のRADIUSサーバとの通信に関するトレースメッセージで、以下の2種類のメッセージがあります。

radiusd:パケットタイプ:識別子,レングス(IPアドレス)(ユーザ名)
radiusd:パケットタイプ:識別子,レングス(IPアドレス) 応答時間

各トレースメッセージのパラメータの意味は、以下のとおりです。

パケットタイプ

： RADIUSパケットのパケットタイプ

REQ	：	認証要求(AccessRequest)
REQ-RS	：	認証要求の再送
ACT	：	認証成功(AccessAccept)
REJ	：	認証拒否(AccessReject)
CHA	：	チャレンジ要求(AccessChallenge) (本装置ではサポートしていません)

識別子

： 送受信しているRADIUSパケットの識別子が表示されます。

レングス

：送受信しているRADIUSパケットのパケット長（バイト数）が表示されます。

IPアドレス

：通信しているRADIUSサーバのIPアドレスが表示されます。

ユーザ名

：RADIUSパケット内のユーザ名（User-Name）が表示されます。

応答時間

：本装置がRADIUS認証サーバにRADIUSパケット(REQ,REQ-RS)を発行してから、RADIUS認証サーバから応答が返ってくるまでの時間（単位：ms ）が表示されます。

(3) acctd トレースメッセージのフォーマット

acctd トレースメッセージは、アカウント時のRADIUSサーバとの通信に関するトレースメッセージで、以下の２種類のメッセージがあります。

acctd:パケットタイプ:識別子,レングス(IPアドレス)(ステータスタイプ,ユーザ名)
acctd:パケットタイプ:識別子,レングス(IPアドレス) 応答時間

各トレースメッセージのパラメータの意味は、以下のとおりです。

パケットタイプ

：RADIUSパケットのパケットタイプ

REQ	：アカウント要求（AccountingRequest）
REQ-RS	：アカウント要求の再送
RSP	：アカウント応答（AccountingResponse）

識別子

：送受信しているRADIUSパケットの識別子が表示されます。

レングス

：送受信しているRADIUSパケットのパケット長（バイト数）が表示されます。

IPアドレス

：通信しているRADIUSサーバのIPアドレスが表示されます。

ステータスタイプ

：RADIUSパケット内のアカウントステータスタイプ（Account-Status-Type）の情報

START	：Account-Status-Type がStart のRADIUSパケット
STOP	：Account-Status-Type がStop のRADIUSパケット

ユーザ名

：　RADIUSパケット内のユーザ名（User-Name）が表示されます。

応答時間

：　本装置がRADIUSアカウントサーバにRADIUSパケット(REQ,REQ-RS)を発行してから、RADIUSアカウントサーバから応答が返ってくるまでの時間（単位：ms ）が表示されます。

■ DSPトレースメッセージ

これは、DSPを使用して処理が行われるモデム通信およびPIAFS通信に関連するトレースメッセージです。

(1) 表示例

本装置のコンソールに表示されるトレースメッセージの表示例を以下に示します。

モデム通信の開始から終了までのトレースメッセージの表示例

```
@T(8/30 12.47.05):[CID 2001]:DSPC(3-1):C1-2-1:START(MODEM)
@T(8/30 12.47.28):[CID 2001]:DSPC(3-1):C1-2-1:CONNECT(MODEM,V90,49333,LAPM,V42BIS)
@T(8/30 12.52.36):[CID 2001]:DSPC(3-1):C1-2-1:STOP(MODEM)
```

PIAFS通信の開始から終了までのトレースメッセージの表示例

```
@T(8/30 12.36.16):[CID 5015]:DSPC(4-22):C1-5-22:START(PIAFS)
@T(8/30 12.36.16):[CID 5015]:DSPC(4-22):C1-5-22:CONNECT(PIAFS,V2.1,64000)
@T(8/30 12.45.25):[CID 5015]:DSPC(4-22):C1-5-22:STOP(PIAFS)
```

(2) トレースメッセージのフォーマット

DSPのトレースメッセージには、以下の3種類のメッセージがあります。

[CID ****]:DSPC(P1):P2:START(通信種別)
[CID ****]:DSPC(P1):P2:STOP(通信種別)
[CID ****]:DSPC(P1):P2:CONNECT(通信種別、プロトコル、送信速度、データプロトコル、圧縮プロトコル)

各トレースメッセージのパラメータの意味は、以下のとおりです。

P1：識別情報1

(m-n)
m ：DSPを収容しているDSPボードのスロット番号
n ：DSP番号

P2：識別情報2

・NS-4200-10の場合
(Cw-x-y-z)
w ：DSPCが動作しているDSPボードのスロット番号
x ：発着信したPRIボードのスロット番号
y ：発着信したPRIボードのポート番号
z ：発着信したPRIポートのBチャネル番号

・NS-4200-30の場合

(Cx-y-z)

x ：発着信したPRIボードのスロット番号

y ：発着信したPRIボードのポート番号

z ：発着信したPRIポートのBチャネル番号

通信種別

： 通信種別を示します。

MODEM ：モデム通信の場合

PIAFS ：PIAFS通信の場合

START

： 接続処理を開始したことを示します。

STOP

： 通信が終了したことを示します。

CONNECT

： モデムあるいはPIAFSのコネクションが確立したことを示します。

プロトコル

： 接続に使用されたプロトコルが表示されます。
通信種別がMODEMの場合には、V90、K56FLEX、V34、V32BISが表示されます。
通信種別がPIAFSの場合には、V1.0、V2.0、V2.1が表示されます。

送信速度

： 確立したモデムあるいはPIAFSのコネクションにおける送信速度（単位：bps）が表示されます。

データプロトコル

： 通信種別がMODEMの場合のみ、使用されているデータプロトコル（LAPM／MNP／DIRECT）が表示されます。

圧縮プロトコル

： 通信種別がMODEMの場合のみ、使用されている圧縮プロトコル（V42BIS／MNP5／NONE）が表示されます。

付録C

RADIUSサーバについて

付録Cでは、本装置がサポートしているRADIUS認証サーバにおけるattributeの設定方法、および本装置がRADIUSアカウントサーバに送信するattributeについて説明しています。

本章の内容

C.1　RADIUS認証サーバから受信可能なattribute

本装置が接続相手を認証する場合、まずローカルデータベース（本装置のusersファイル）を検索します。接続相手の情報が本装置のローカルデータベースに登録されてなく、かつ本装置のradiusファイルでRADIUS認証サーバを使用するモードに設定されている場合には、指定されたRADIUS認証サーバに認証要求（AccessRequestパケット）を送信します。

RADIUS認証サーバにおける認証が成功すると、認証成功のパケット（AccessAcceptパケット）を受信します。その後の接続相手の動作条件は、受信した認証成功パケットに含まれているattribute情報に基づきます。

本装置がRADIUS認証サーバから受信する認証成功パケットのattributeの解釈方法を、**表C-1**に示します。なお、表**C-1**に示すattribute以外のattributeを受信した場合、本装置で廃棄されます。

表C-1　RADIUS認証サーバから受信するAccessAcceptの解釈方法　**(1/2)**

Attribute名	番号	Attributeの定義	可能な設定値／設定方法 (＊1)
Service-Type	6	ユーザが要求しているサービスタイプ	2：Framed-User　通常の着信ユーザの場合に指定します。 4：Callback-Framed-User PPPのCBCPでCallbackするユーザの場合に指定します。
Framed-Protocol	7	FramedAccessに使用されるFraming	1：PPP　PPPを指定します。（＊2）
Framed-IP-Address	8	ユーザに設定されるIPアドレス	PPPのIPCPで行うアドレスネゴシエーションの動作を設定します。 255.255.255.255：相手の通知してくるIPアドレスを受け入れる。 255.255.255.254：本装置のIPプールのアドレスを相手のIPアドレスとして使用する。 上記以外：設定されたアドレスを相手IPアドレスとして使用する。 この情報をもとに本装置のusersファイルのinterfaceキーワードの設定を自動生成します。(＊3)
Filter-Id	11	ユーザに対するfilter名	Framed-IP-Addressの内容をもとに自動生成される本装置usersファイルのinterfaceキーワードに対するfilter名を設定します。filter名の後ろに「.」で区切り、拡張子を設定できます。filter名は本装置のipfiltersファイルに設定されている必要があります。 拡張子filterの場合あるいは拡張子なしの場合 (例：filA.filter) 「filter　filA」と解釈されます。 拡張子includeの場合 (例：filA.include) 「access include　filA」と解釈されます。 拡張子excludeの場合 (例：filA.exclude) 「access exclude　filA」と解釈されます。 拡張子outputfilの場合 (例：filA.outputfil) 「outputfil　filA」と解釈されます。（＊3）
Callback-Number	19	コールバックする電話番号	コールバックする電話番号を指定したい場合に、電話番号を設定します。区切り記号として、「-」を使用できます。
Framed-Route	22	ユーザに設定されるルーティング情報	以下の書式で設定します。 destination/mask　gateway　metric　[filter名] destination：宛先アドレスを設定 mask：destinationのマスクを10進数で設定 gateway：宛先に到達するために経由するルータのIPアドレスを設定 metric：このルートのメトリックを10進数で設定 filter：このルートに対するフィルタを設定する場合には、filter名を設定(filter名は本装置のipfiltersファイルに設定されている必要があります) この情報をもとに、本装置usersファイルのdestinationキーワードの設定を自動生成します。(＊4)

表C-1　RADIUS認証サーバから受信するAccessAcceptの解釈方法

(2/2)

Attribute名	番号	Attributeの定義	可能な設定値／設定方法 (＊1)
Session-Timeout	27	sessionの終了までにユーザに提供されるサービスの最大時間	5～100000 (秒) が有効 0の場合は自動切断を行いません。
Idle-Timeout	28	sessionの終了までにユーザに許される最大連続idle時間	5～100000 (秒) が有効 0の場合は自動切断を行いません。
Port-Limit	62	ユーザが使用できる最大リンク数	MPプロトコルで動作時に、使用できる最大リンク数を設定します。 設定範囲:1～8
Assign-IP-Pool	218	ユーザが使用するIPプール番号	ippool ファイルに登録しているプール番号(設定範囲:1～16)を指定します。この値が0の場合、ippoolファイルに登録されているすべてのIPプールから空いているIPアドレスを検索して、空いているIPアドレスを割り当てることができます。 (＊5)

(＊1)　RADIUS認証サーバに設定する場合、設定値（たとえばFramed-Userなどの書式、設定値) は、ご使用になるRADIUS認証サーバで異なる場合がありますので、使用されるRADIUS認証サーバの設定ファイル (たとえばusersファイル、dictionaryファイルなど) を確認してください。

(＊2)　MPで接続する場合にも、PPPを指定します。その場合、MPの最大リンク数をPort-Limitで設定します。

(＊3)　Framed-IP-Address、Filter-Idの設定をもとに、本装置usersファイルの「%user」に設定するinterfaceキーワードの設定を本装置内部で自動生成します。以下にいくつかの例を示します。

Framed-IP-Address／Filter-Idの設定	自動生成されるinterfaceキーワードの内容
なしの場合、あるいは 255.255.255.254	interface　isdn0　　*　unnumbered 　ppp address　　on　*　255.255.255.254
255.255.255.255	interface　isdn0　　*　unnumbered 　ppp address　　on　*　255.255.255.255
上記以外 (たとえば10.0.0.1の場合)	interface　isdn0　　10.0.0.1　unnumbered 　ppp address　　on　*　10.0.0.1
10.0.0.1で以下のfilter-Idが設定されている場合 Filter-Id　filA.filter Filter-Id　filB.include	interface　isdn0　　10.0.0.1　unnumbered 　ppp address　　on　*　10.0.0.1 　filter　　filA 　access include　filB

(＊4)　Framed-Routeの設定をもとに、本装置usersファイルの「%user」に設定するdestinationキーワードの設定を本装置内部で自動生成します。以下にいくつかの例を示します。

Framed-Routeの設定	自動生成されるdestinationキーワードの内容
128.30.0.0/16　128.30.1.1　2	destination 128.30.0.0/16　via 128.30.1.1　2
128.30.0.0/16　128.30.1.1　2　filA	destination 128.30.0.0/16　via 128.30.1.1　2 　filter　　filA

(＊5)　RADIUS認証サーバによってはこのattributeが定義されていない場合があります。
その場合には、RADIUS認証サーバのdictionaryに、Assign-IP-Poolを番号「218」、データ形式「integer」で登録してください。

本装置では、受信したattribute情報から、本装置のusersファイルにおけるキーワードにマッピングします。したがって、attribute情報で指定されない動作条件は、そのattributeのデフォルト値が使用されます。
RADIUS認証サーバで、ユーザ名およびパスワードのみ設定し、attributeを設定しない場合には、本装置では以下のようにRADIUS認証サーバで指定された場合と同様に動作します。（「RADIUS認証サーバのusersファイル設定例1」と「RADIUS認証サーバのusersファイル設定例2」は同等になります）

RADIUS認証サーバのusersファイルの設定例1

```
sii   Password = “siipassword”
```

RADIUS認証サーバのusersファイルの設定例2

```
sii   Password = “siipassword”
      Service-Type       = Framed-User,
      Framed-Protocol    = PPP,
      Framed-IP-Address  = 255.255.255.254,
      Idle-Timeout       = 120
```

注 意　本装置では、アイドル監視機能がデフォルトでは有効になっており、アイドル監視時間は120秒です。アイドル監視を行わない場合には、本装置のusersファイルの%defalut分類キーワードに、以下の設定を追加してください。

アイドル監視を行わない場合の本装置usersファイルの設定

```
%default
      auto_disconnect    off
```

また、すべての接続相手共通にアイドル監視時間を設定したい場合にも、本装置のusersファイルの%default分類キーワードに設定することによって、RADIUS認証サーバに設定しなくてもアイドル監視時間を設定することができます。たとえば、アイドル監視時間を3600秒（1時間）にしたい場合には、以下のように設定します。

アイドル監視を1時間で行う場合の本装置usersファイルの設定

```
%default
      auto_disconnect    on
      idle_timeout       3600
```

なお、この設定をした場合でも、RADIUS認証サーバにおいてIdle-Timeoutの設定を行った場合には、RADIUS認証サーバの設定が有効になります。

C.2　RADIUSアカウントサーバに送信するattribute

本装置がRADIUSアカウントサーバに送信するattributeを以下に示します。

表C-2　RADIUSアカウントサーバに送信するattribute

Attribute名	番号	AccountStartに含まれるattribute	AccountStopに含まれるattribute
User-Name	1	○	○
NAS-IP-Address	4	○	○
NAS-Port	5	○	○
Service-Type	6	○	○
Framed-Protocol	7	○	○
Framed-IP-Address	8	○	○
Callback-Number (*1)	19	○	○
Session-Timeout (*2)	27		○
Idle-Timeout (*2)	28		○
Called-Station-Id (*3)	30	○	○
Calling-Station-Id (*4)	31	○	○
Acct-Status-Type	40	○	○
Acct-Delay-Time	41	○	○
Acct-Input-Octets	42		○
Acct-Output-Octets	43		○
Acct-Session-Id	44	○	○
Acct-Authentic	45	○	○
Acct-Session-Time	46		○
Acct-Input-Packets	47		○
Acct-Output-Packets	48		○
Acct-Terminate-Cause	49		○
Acct-Multi-Session-Id (*5)	50	○	○
Acct-Link-Count (*5)	51	○	○
NAS-Port-Type	61	○	○
Connect-Info (*6)	77	○	○
Acct-Disconnect-Cause (*7)	195		○

(*1)　コールバックの場合のみ、このattributeを送信します。
(*2)　機能が指定された場合のみ、このattributeを送信します。
(*3)　着信の電話番号が通知されてきた場合のみ、このattributeを送信します。
(*4)　発信者の電話番号が通知されてきた場合のみ、このattributeを送信します。
(*5)　MPで接続された場合のみ、このattributeを送信します。
(*6)　RADIUSアカウントサーバによっては、Connect-Infoが定義されていない場合があります。その場合にはdictionaryファイルに、Connect-Infoを番号「77」、データ形式「string」で定義してください。
またLivingston2.0.1 の dictionary には、Connect-Info が 番号「65」で定義されています。この場合には、この値を番号「77」に変更してRADIUSサーバを再起動してください。
(*7)　radiusファイルの%radius_acct分類キーワードに「disconnect_cause on」を設定した場合のみ、このattributeを送信します。
RADIUSアカウントサーバによっては、Acct-Disconnect-Causeが定義されていない場合があります。その場合にはdictionaryファイルに、Acct-Disconnect-Causeを番号「195」、データ形式「integer」で定義してください。
dictionary変更後は、RADIUSサーバを再起動してください。

表C-2におけるRADIUSアカウントサーバに送信する各attributeの意味と、本装置が格納する内容について、**表C-3**に示します。

表C-3　RADIUSアカウントサーバへ送信するattributeの内容

(1 / 3)

Attribute名	番号	内　　容
User-Name	1	認証されるユーザ名
NAS-IP-Address	4	ユーザの認証を要求している本装置のIPアドレス 本装置のホスト名に対応するIPアドレスが使用されます。
NAS-Port	5	ユーザを認証している本装置の物理ポート番号 swcc　s:　拡張ボードスロット番号 w:　PRIポート番号 cc:　Channel番号　01-23
Service-Type	6	ユーザが要求しているサービスタイプ 2:Framed-User 4:Callback-Framed-User
Framed-Protocol	7	FramedAccessに使用されるFraming 1:PPP
Framed-IP-Address	8	ユーザに設定されるIPアドレス
Callback-Number	19	コールバックする電話番号
Session-Timeout	27	sessionの終了までにユーザに提供されるサービスの最大時間 （単位：秒）
Idle-Timeout	28	sessionの終了までにユーザに許される最大連続idle時間（単位：秒）
Called-Station-Id	30	通知されてきた着信電話番号
Calling-Station-Id	31	通知されてきた発信者の電話番号
Acct-Status-Type	40	アカウントログの種別 ユーザのサービス開始、終了を記録します。 1:Start 2:Stop
Acct-Delay-Time	41	アカウントが発生してからの遅延時間。０以外の場合アカウントの再送が発生したことを表します。
Acct-Input-Octets	42	受信したデータ量をオクテット数で表示
Acct-Output-Octets	43	送信したデータ量をオクテット数で表示
Acct-Session-Id	44	セッションID。StartとStopを関連づけます。 8桁のHEXで表示します。上位8桁は本装置が再起動する度に更新されます。
Acct-Authentic	45	ユーザの認証の仕方 1:RADIUS 2:Local
Acct-Session-Time	46	ユーザがサービスを受けた時間（単位 : 秒）
Acct-Input-Packets	47	受信したデータ量をパケット数で表示
Acct-Output-Packets	48	送信したデータ量をパケット数で表示

表C-3　RADIUSアカウントサーバへ送信するattributeの内容

(2 / 3)

Attribute名	番号	内　　容
Acct-Terminate-Cause	49	切断理由 1:User-Request 　　ユーザからの切断要求による切断 4:Idle-Timeout 　　アイドルタイムアウトによる切断 5:Session-Timeout 　　セッションタイムアウトによる切断 6:Admin-Reset 　　本装置の管理者による切断 12:Port-Unneeded 　　BODの帯域制御で不要と判断して切断 13:Port-Preempted 　　本装置が優先度の高い用途に割り当てるために切断 14:Port-Suspended 　　disableのポートに着呼したために切断 15:Service-Unavailable 　　ユーザが要求するサービスを本装置が提供できないために 　　切断 16:Callback 　　コールバックのための切断
Acct-Multi-Session-Id	50	MP接続時のセッションID
Acct-Link-Count	51	MP接続時のリンクカウント数
NAS-Port-Type	61	ユーザを認証している回線サービスのタイプ 　　0:Async 　　2:ISDN-Sync 　　6:PIAFS　(*1)
Connect-Info	77	接続速度（送信速度/受信速度）とその他情報 （例） ・ISDN(同期64K)接続時 　　　"64000/64000" ・モデム接続時 　変調プロトコル 　ITU-TV.90　"48000/28800 V90 LAPM V42BIS" 　K56flex　"44000/28800 K56FLEX LAPM V42BIS" 　ITU-TV.34　"33600/31200 V34 LAPM V42BIS" ・PIAFS(32K)接続時 　　　"32000/32000 PIAFS V1.0"

(*1)　RADIUSアカウントサーバによっては、NAS-Port-Typeの「PIAFS」が定義されていない場合があります。その場合には、dictionaryファイルに「PIAFS」を値「6」で登録してください。

表C-3　RADIUSアカウントサーバへ送信するattributeの内容

(3 / 3)

Attribute名	番号	内　　容
Acct-Disconnect-Cause	195	切断理由 2: 下記の切断理由以外による切断 11: MODEM/PIAFSの接続に成功した後、MODEM/PIAFSが切断 42: PAP認証に失敗したことによる切断 43: CHAP認証に失敗したことによる切断 45: PPPセッション確立後、接続相手からのLCPのTerminate-Request受信による切断 100: PPPセッション確立後、アイドルタイムアウトによる切断 151: 本装置の管理者による切断 185: ISDNが確立した後、ISDNが切断 195: PPPセッション確立後、セッションタイムアウトによる切断

C.3　RADIUSサーバ側の設定例

ここでは、Livingston社のRADIUSサーバを使用した場合の設定例をいくつか説明します。

C.3.1　RADIUSサーバのclientsファイルの設定例

本装置とRADIUSサーバとが通信できるようにするためには、お互いの情報を設定する必要があります。

RADIUSサーバの設定では、本装置のIPアドレス、本装置と共通にもつsecretキーを設定します。Livingston社のRADIUSサーバではこの情報をclientsファイルに登録します。

RADIUSサーバのclientsファイルの設定例

```
#Client Name         Key
ns4200               ns4200secret
```

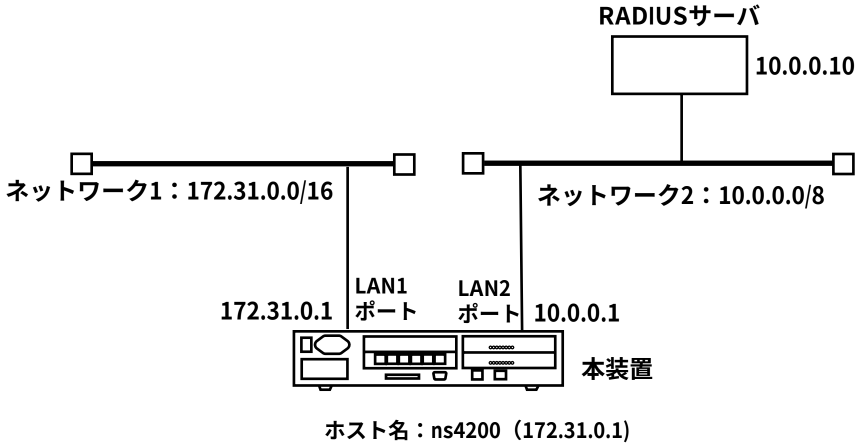
RADIUSサーバのhostsファイルの設定例

```
172.31.0.1           ns4200
```

clientsファイルの最初のフィールドには、本装置のホスト名かIPアドレスを指定します。次のフィールドには、本装置と共通にもつsecretキーを指定します。
clientsファイルに設定する本装置のIPアドレスは、本装置のホスト名のIPアドレスを指定します。clientsファイルを変更した場合は、RADIUSサーバの再起動が必要です。

注 意　**本装置がRADIUSサーバに送信するRADIUSサーバパケットのソースIPアドレスおよび「NAS-IP-Address」attributeには、本装置のホスト名に対応するIPアドレスが使用されます。**

**例えば、LAN2ポート側にRADIUSサーバ（10.0.0.10）を設置した場合を考えます。この場合、RADIUSサーバ（10.0.0.10）のclientsファイルに登録する本装置のIPアドレスは、ホスト名に対応するIPアドレス172.31.0.1でなければなりません（10.0.0.1ではありません）。
また、本装置のホスト名に対応するIPアドレス172.31.0.1に対するルートをRADIUSサーバ(10.0.0.10)に設定する必要があります。
この場合、RADIUSサーバに設定する172.31.0.1に対するルートのゲートウェイは、本装置のLAN2ポートのIPアドレス10.0.0.1を指定します。**



本装置の設定は、radiusファイルに登録します。
RADIUSサーバを使用するために、modeキーワードをonに設定します。
さらに、RADIUSサーバのIPアドレス、RADIUSサーバのUDPのポート番号、RADIUSサーバと共通にもつsecretキーを設定します。（**「5.11　radiusファイル」**参照）

C.3.2　RADIUS認証サーバのusersファイルの設定例

ここでは、RADIUS認証サーバにおけるusersファイルの設定例をいくつか説明します。

(1) 端末型PPP接続

PPPで端末型接続を行う場合の設定例です。接続条件は、

- ユーザ名はsii、パスワードはsiipassword
- IPアドレスを本装置のIPプールから割り当てる
- 3600秒(１時間)無通信状態が続いた場合、自動的に切断する

の場合です。

```
sii Password = "siipassword"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 255.255.255.254,
  Idle-Timeout = 3600
```

(2) 端末型MP接続

MPで端末型接続を行う場合の設定例です。接続条件は、

- ユーザ名はsii、パスワードはsiipassword
- IPアドレスを本装置のIPプールから割り当てる
- ユーザが使用できる最大リンク数は２

の場合です。

```
sii Password = "siipassword"
  Service-Type = Framed-User,
  Framed-Protocol = PPP,
  Framed-IP-Address = 255.255.255.254,
  Port-Limit = 2
```

なお、MPの着信を許可するためには、本装置の着信時に受け入れるプロトコル(本装置のusersファイルの%presetのprotocol)をmpに設定する必要があります（「**4.4.4　MPを使用する場合の設定**」参照）。

(3) CBCPコールバック接続

PPPのCBCPでコールバックを行う場合の設定例です。接続条件は、

- ユーザ名はcbsii、パスワードはsiipassword
- Callbackを許可する
- コールバックする電話番号は、03-1111-1111
- IPアドレスを本装置のIPプールから割り当てる

の場合です。

```
cbsii Password = "siipassword"
      Service-Type = Callback-Framed-User,
      Framed-Protocol = PPP,
      Framed-IP-Address = 255.255.255.254,
      Callback-Number = "03-1111-1111"
```

本装置がコールバック要求を受け入れてコールバックする場合、次のどちらかの相手電話番号を使用します。

- Callback-Number attributeで設定された相手電話番号。
- 着信時に、発信者番号通知で通知された相手電話番号。

両方とも有効な場合（Callback-Numberが設定され、かつ発信者番号が通知された場合）は、Callback-Number attributeで設定された電話番号が優先されます。
両方とも無効な場合は、接続相手に対して、CBCPのプロトコルを使用してコールバックする電話番号の問い合わせを行い、相手から通知された電話番号にコールバックします。

(4) 端末型PPP接続でPPP認証時に発信者電話番号をチェックする場合

PPPで端末型接続を行い、かつ発信者の電話番号もチェックする場合の設定例です。
接続条件は、

- ユーザ名はsii、パスワードはsiipassword
- IPアドレスを本装置のIPプールから割り当てる
- 発信者の電話番号が03-2222-2222のユーザのみ接続を許可する

の場合です。

```
sii Password = "siipassword",Calling-Station-Id="0322222222"
    Service-Type = Framed-User,
    Framed-Protocol = PPP,
    Framed-IP-Address = 255.255.255.254
```

(5) 端末型PPP接続でISDN着信時に発信者電話番号をチェックする場合

ISDN着信時にCLID認証（通知されてきた発信者電話番号による認証）を行う場合の設定例です。

接続条件は、

- 発信者の電話番号が03-1111-1111のユーザのみ接続を許可する
- IPアドレスを本装置のIPプールから割り当てる

の場合です。

```
0311111111   Password = "siipassword",Service-Type = Call-Check
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 255.255.255.254
```

ISDN着信時にCLID認証を行う場合、本装置は、以下に示す値で、RADIUS認証サーバに認証要求（AccessRequestパケット）を送信します。

User-Name ：通知されてきた発信者の電話番号で送信します。

Password ：“ siipassword ” で送信します。
このパスワードを変更したい場合は、本装置のradiusファイルの%radius_auth分類キーワードのext_passwdキーワードで設定できます（**「5.11　radiusファイル」**参照）。

Service-Type ：Call-Check で送信します。

なお、この設定を有効にするためには、本装置をISDN着信時にCLID認証を行うモードに設定（本装置のusersファイルの%preset分類キーワードのclid_authキーワードをmayかmustに設定）し、かつRADIUS認証サーバを使用してCLID認証を行うモードに設定（本装置のradiusファイルの%radius_auth分類キーワードのclid_authキーワードをonに設定）する必要があります（**「4.4.2　CLID認証を使用する場合の設定」**参照）。

注 意　**RADIUS認証サーバによっては、Service-Type attributeの値「Call-Check」が定義されていない場合があります。その場合にはdictionaryファイルのService-Type attributeの値を定義している部分に「Call-Check」を値「10」で追加してください。**

C.4 RADIUS アカウントサーバのアカウントログの記述例

本装置がISDNでPPP接続を行った場合に、RADIUSアカウントサーバ(DTCのRADIUSサーバ：version2.03)のdetailファイルに記述されるアカウントログの例を以下に示します。

```
Thu Aug  5 08:52:10 1999
        Acct-Status-Type = Start
        NAS-IP-Address = 172.31.2.192
        NAS-Port = 1119
        NAS-Port-Type = ISDN-Sync
        Calling-Station-Id = "1234567890"
        User-Name = "sii"
        Acct-Session-Id = "02000003"
        Service-Type = Framed-User
        Acct-Authentic = RADIUS
        Framed-Protocol = PPP
        Framed-IP-Address = 172.31.203.64
        Connect-Info = "64000/64000"
        Acct-Delay-Time = 0

Thu Aug  5 08:53:08 1999
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.31.2.192
        Acct-Terminate-Cause = User-Request
        Acct-Session-Time = 59
        NAS-Port = 1119
        NAS-Port-Type = ISDN-Sync
        Calling-Station-Id = "1234567890"
        User-Name = "sii"
        Acct-Session-Id = "02000003"
        Service-Type = Framed-User
        Acct-Authentic = RADIUS
        Framed-Protocol = PPP
        Acct-Input-Octets = 5068
        Acct-Output-Octets = 790
        Acct-Input-Packets = 61
        Acct-Output-Packets = 12
        Framed-IP-Address = 172.31.203.64
        Session-Timeout = 86400
        Idle-Timeout = 3600
        Connect-Info = "64000/64000"
        Acct-Delay-Time = 0
```

付録D

TELNETサーバの設定

付録Dでは、TELNETサーバの設定方法について説明しています。

本装置のTELNETサーバへのログインを制限することができます。
制限としては、同時ログイン数、接続できるローカルおよびリモートアドレスがあります。これらの制限はserversファイルに設定して、リブートすると有効になります。

serversファイル（TELNETサーバ制限なし）

```
        :
/share/telnetd  -CON
```

serversファイル（TELNETサーバ制限つき）

```
        :
/share/telnetd -CON -s 1 -l routerA -r hostX
```

自局ホスト名　**相手ホスト名**

同時ログイン数：
TELNETで本装置に同時にログインできるユーザ数をキーワード（-s）のあとにスペースをあけて指定します。指定できる値は１から５です。

自局ホスト名：
本装置が複数の自局IPアドレスを持っているときに、そのうちの1つのIPアドレスに対応するホスト名をキーワード（-l）の後にスペースをあけて指定します。TELNETクライアントからはこのアドレスでしか接続できなくなります。「＊」を指定するとhostnameファイルに設定したホスト名が使われます。

相手ホスト名：
本装置のTELNETサーバに接続できるTELNETクライアントのホスト名をキーワード（-r）の後にスペースをあけて指定します。このホスト名に対応するアドレスを持った装置のみがTELNETサーバに接続できます。

付録E

バージョンアップ手順

付録Eでは、本装置のシステムソフトウェアのバージョンアップ手順、本装置のシステムソフトウェアのバックアップ手順、本装置のシステムソフトウェアのリストア手順について説明しています。

本章の内容

E.1　システムソフトウェアのバージョンアップ

本装置のシステムソフトウェアのバージョンアップ方法を説明します。
バージョンアップ手順は以下のようなステップで行います。

・ バージョンアップ
・ 新規バージョンでの立ち上げ

現行バージョンのシステムソフトウェアのバックアップを行う場合には、事前に**「E.2　システムソフトウェアのバックアップ」**を行ってから、バージョンアップを実施してください。

使用するバージョンアップファイルは現行のバージョンと新規バージョンの組み合わせにより異なります。ファイルの入手方法などは、弊社サポート窓口までお問い合わせください。
本装置にバージョンアップ用のFTPサーバ（以下、バージョンアップサーバと呼ぶ）を立ち上げておくことにより、UNIXなどのFTPクライアントからLANやWANを介してシステムソフトウェアのバージョンアップが行えます。

バージョンアップの手順を以下に示します。

(1) バージョンアップサーバの立ち上げ

バージョンアップサーバが起動するように、serversファイルを設定します。デフォルトではバージョンアップサーバが立ち上がるように設定されていません。バージョンアップサーバを立ち上げる場合には、serversファイルの/share/vupdの行を有効にして、リブートしてください。

serversファイル（バージョンアップサーバの起動）

```
      :
/share/vupd
```

オプションとして、バージョンアップサーバにログインできる自局および相手のホスト名（hostsファイルに設定している名前）を指定することができます。自局または相手のホスト名はどちらか一方のみを指定することもできます。

serversファイル（ローカル／リモートホスト名の指定）

```
      :
/share/vupd  -l  localhost  -r  remotehost
```

自局ホスト名　相手ホスト名

自局ホスト名

：本装置が複数の自局IPアドレスを持っているときに、そのうちの一つのIPアドレスに対応するホスト名をキーワード（-l）の後にスペースをあけて指定します。FTPクライアントからはこのアドレスでしか接続できなくなります。
ホスト名に「*」を指定すると、hostnameファイルに指定したホスト名が使用されます。

相手ホスト名

：本装置のバージョンアップサーバに接続できるFTPクライアントのIPアドレスに対応するホスト名をキーワード（-r）の後にスペースをあけて指定します。このIPアドレスを持った装置のみがバージョンアップサーバに接続できます。

(2) バージョンアップ用ユーザの追加

バージョンアップ用のバージョンアップサーバにログインできるのは、ユーザID=99のユーザのみです。
バージョンアップをする際には、authコマンドでユーザID＝99のユーザを追加します。さらに、このユーザでログインしてパスワードを設定します。

```
# auth  add  verup  99↓        ID=99のユーザを追加
# telnet  routerA↓
login: verup↓                  追加したユーザでログイン
passwd: _↓
routerA> passwd↓               パスワードの設定
Enter New Password ?_↓
Re-Enter New Password ?_↓
routerA> lo↓
# write↓                       必要ならば設定を保存する
```

注　意　　**パスワードが設定されていないと、バージョンアップサーバにはログインできません。**

(3) 新しいOSの転送

新しいバージョンのシステムソフトウェア（ファイル名：system）をUNIXワークステーションなどに用意します。FTPクライアントから**(2)**で設定したユーザ名およびパスワードで本装置にログインします。

注　意　　**新しいバージョンのシステムソフトウェアの入手方法については、お買い上げになった代理店などにご相談ください。**

注　意　　**以下の説明中のコマンドは、使用するFTPクライアントの種類により異なります。詳細は使用するFTPクライアントのマニュアルを参照してください。**

FTPをバイナリ転送モードに設定します（コマンド「binary」）。
新しいシステムソフトウェアを転送します（コマンド「put　system」）。

```
1 mk > ftp 130.111.1.122↓
Connected to 130.111.1.122.
220 version up server ready.
Name (130.111.1.122:ftp):verup↓     ID=99のユーザでログインする
331 User name ok,need password.
Password:____↓
230 User logged in.
ftp> binary↓                        バイナリモードにする
200 Type set to I.
ftp> put  system↓                   システムソフトウェアの転送
200 PORT command ok.
150 Binary data connection for system.
226 Binary Transfer complete.
local: system remote: system
2727936 bytes sent in 1.2e+02 seconds (21 Kbytes/s)
ftp> bye↓
221 Good bye.
2 mk >
```

もし、通信障害などで転送が失敗した場合には、再度、転送を実行してください。

注　意　　**ファイルの転送中に電源を切ったり、RESETスイッチを押さないでください。システムソフトウェアが立ち上がらなくなります。**

(4) 新規バージョンの起動

rebootコマンドを実行すると、通常のリブートと異なり旧バージョンから新規バージョンへのファイルの置き換えが行われ、新規バージョンのシステムソフトウェアが既存のセットアップで立ち上がります。そのため、通常のリブートよりも起動するまでに時間がかかります。

CONSOLEポートの表示例

```
# reboot↓
Do you really want to reboot [y/n] ?  y↓

BOOT...
system new image found...

BOOT...
     （以下、起動時のメッセージが表示されます）
```

注　意　　ファイルの置き換え中に電源を切ったり、RESETスイッチを押さないでください。システムソフトウェアが立ち上がらなくなります。

注　意　　telnetでログインしている場合には、rebootコマンドを実行すると切断されます。システムソフトウェアが立ち上がるのを待ってから、再度ログインしてください。

注　意　　新規バージョンでセットアップファイルが追加されている場合には、clear -upコマンドを実行してファイルを追加して、writeコマンドで保存してください。clear -upを実行しても新規セットアップファイルを追加するだけです。既存の設定は保存されています。

```
# clear -up↓
        （追加されたファイル名が表示されます）
# write↓
```

本装置が起動したら、以下のようにconsoleコマンドを実行して、立ち上がり時のメッセージでバージョンの確認、およびエラーメッセージが表示されていないかの確認をしてください。また通信やその他の機能が正常であることを確認してください。正常であればバージョンアップは終了です。

```
# console –rev 10000↓

   （起動時のメッセージが表示されます）
```

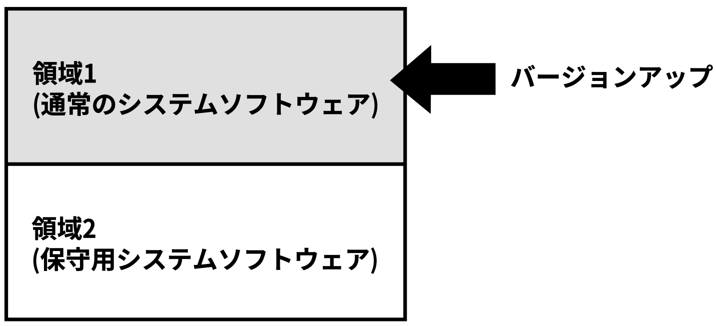
E.2　システムソフトウェアのバックアップ

ここでは、本装置の現行バージョンのシステムソフトウェアのバックアップについて説明します。システムソフトウェアのバックアップには、およそ24MBのファイル転送が必要ですので、ローカルLANや高速回線で行うことを推奨します。
バックアップしたシステムソフトウェアは、**「E.3　システムソフトウェアのリストア」**の手順によって、再度インストールすることができます。

まず、システムソフトウェアのバックアップ方法の説明を行う前に、本装置のシステムソフトウェアの構成について簡単に説明します。
本装置のシステムソフトウェアは、内蔵のメモリに格納されています。内蔵メモリは、以下の２つの領域に分かれています。

領域1　：　通常使用するシステムソフトウェアの格納領域
この領域には通常運用で使用するシステムソフトウェアが格納されています。システムソフトウェアのバージョンアップは、この領域に対して行われます。

領域2　：　保守用システムソフトウェアの格納領域
この領域には、出荷時に保守用システムソフトウェアが格納されています。



＜本装置の内蔵メモリのイメージ図＞

したがって、システムソフトウェアのバックアップ／リストアを行う対象は、通常使用するシステムソフトウェアが格納されている領域1のシステムソフトウェアになります。
またシステムソフトウェアのバックアップあるいはリストアは、領域2の保守用システムソフトウェアで本装置を起動した状態で、領域1に格納されているシステムソフトウェアをバックアップ／リストアを行う必要があります。

次に、システムソフトウェアをバックアップする手順を説明します。
まず、領域2の保守用システムソフトウェアを立ち上げ、flftpコマンドを使用してネットワーク上のワークステーションなどにバックアップします。ここで使用するflftpコマンドはFTPクライアントですから、FTPサーバ機能を持ったワークステーションなどが必要です。システムソフトウェアをバックアップするワークステーションにはおよそ24MBのディスクの空き領域が必要です。

(1) 保守用システムソフトウェアの起動

領域1の保守用システムソフトウェアを起動します。

```
# reboot  -p2↓
Do you really want to reboot [y/n] ?  y↓
```

注　意　　**telnetでログインしている場合には、rebootコマンドを実行すると切断されます。保守用システムソフトウェアが立ち上がるのを待ってから、再度ログインしてください。もし、ログインできない場合には、本装置を起動しなおせば現行のシステムソフトウェアが現行のセットアップで立ち上がりますので、セットアップを再度確認してください。**

本装置が起動したら、領域2の保守用システムソフトウェアが立ち上がっていることを確認します。bdinfoコマンドを実行して、以下の表示を確認します。

```
# bdinfo↓
Maintenance system is up.
#
```

注　意　　**もし、“ Normal system is up. ”と表示された場合には、保守用システムソフトウェアが立ち上がっていません。CONSOLEポートに出力されるメッセージの確認および保守用システムソフトウェアの起動をやり直してください。**

(2) システムソフトウェアのバックアップ

保守用システムソフトウェアが起動したら、flftpコマンド（FTPクライアント）を用いて領域1の通常のシステムソフトウェアをワークステーションなどにバックアップします。

flftpコマンドを起動して通常のシステムソフトウェアをバックアップします。ここでは、本装置のシステムソフトウェアをファイル名「backup.img」でバックアップする場合を例に説明します。（このファイル名は、任意の名前でかまいません。）

```
# flftp host1↓
220 host1 FTP server (SunOS 4.1) ready.
login: user1↓
331 Password required for user1.
password: ________↓
230 User user1 logged in.
200 Type set to I.
flftp> put backup.img↓
200 PORT command successful.
150 Binary data connection for backup.img (172.31.3.11,4107).
..........................................（中略）.................................................. complete.
226 Binary Transfer complete.
flftp>quit↓
#
```

注　意　　**バックアップされるシステムソフトウェアは、およそ24MBです。**

注　意　　**上記の例では、flftpコマンド（FTPクライアント）でログインしたディレクトリにシステムソフトウェアがバックアップされます。バックアップするディレクトリを指定する場合には、「put backup.img」の前に「cd xxx/yyy」でディレクトリを変更してください。**

以上でシステムソフトウェアのバックアップは終了です。この状態では、本装置は保守用システムソフトウェアで起動していますので、運用状態に戻すためには、rebootコマンドで本装置を通常のシステムソフトウェアで再起動させる必要があります。

```
# reboot↓
Do you really want to reboot [y/n] ?  y↓
```

E.3　システムソフトウェアのリストア

ここでは、バックアップされている本装置のシステムソフトウェアをリストアする方法について説明します。この手順によって、**「E.2　システムソフトウェアのバックアップ」**の手順でバックアップされているシステムソフトウェアをインストールすることができます。

(1) 保守用システムソフトウェアの起動

「E.2　システムソフトウェアのバックアップ」の(1)と同様の手順で、保守用システムソフトウェアで本装置を起動してください。

(2) システムソフトウェアのリストア

保守用システムソフトウェアが起動したら、ワークステーションなどにバックアップしておいたシステムソフトウェアをflftpコマンド（FTPクライアント）を用いて領域1にリストアします。
ここでは、本装置のシステムソフトウェアをファイル名「backup.img」でバックアップされている場合を例に説明します。

```
# flftp host1↓
220 tai FTP server (SunOS 4.1) ready.
login: user1↓
331 Password required for user1.
password: ________↓
230 User user1 logged in.
200 Type set to I.
flftp> get backup.img↓
Card erase ...........（中略）................................ complete.
200 PORT command successful.
150 Binary data connection for from.img (172.31.3.11,4097) (20971520 bytes).
...................................(中略)................................ complete.
226 Binary Transfer complete.
flftp> quit↓
#
```

注　意　　**上記の例は、flftpコマンド（FTPクライアント）でログインしたディレクトリに「backup.img」がある場合です。異なるディレクトリにシステムソフトウェアが存在する場合には、「get backup.img」の前に「cd xxx/yyy」でディレクトリを変更してください。**

(3) リストアしたシステムソフトウェアの起動

rebootコマンドを実行すると、リストアしたシステムソフトウェアが既存のセットアップで立ち上がります。

```
  # reboot↓
Do you really want to reboot [y/n] ?  y↓

BOOT...

                (以下、起動メッセージが表示されます)
```

注　意　　**telnetでログインしている場合には、rebootコマンドを実行すると切断されます。システムソフトウェアが立ち上がるのを待ってから、再度ログインしてください。**

本装置が起動したら、以下のようにconsoleコマンドを実行して、立ち上がり時のメッセージでバージョンの確認、およびエラーメッセージが表示されていないか確認してください。
通信やその他の機能が正常であることを確認してください。正常であればシステムソフトウェアのリストアは終了です。

```
# console -rev 10000↓

   (起動時のメッセージが表示されます)
```

索引

[L]

[M]

[N]

[P]

[R]

[S]

[T]

[U]

[V]

[W]

[ア]